

2018

Development and Validation of a Proof-of-Concept Prototype for Analytics-based Malicious Cybersecurity Insider Threat in a Real-Time Identification System

Angel L. Hueca

Nova Southeastern University, ahueca@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Angel L. Hueca. 2018. *Development and Validation of a Proof-of-Concept Prototype for Analytics-based Malicious Cybersecurity Insider Threat in a Real-Time Identification System*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1063)
https://nsuworks.nova.edu/gscis_etd/1063.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Development and Validation of a Proof-of-Concept Prototype for Analytics-
based Malicious Cybersecurity Insider Threat in a Real-Time Identification
System

by


Angel L. Hueca

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University


2018

We hereby certify that this dissertation, submitted by Angel Hueca, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.




Yair Levy, Ph.D.
Chairperson of Dissertation Committee

12/6/2018
Date



Michelle M. Ramim, Ph.D.
Dissertation Committee Member

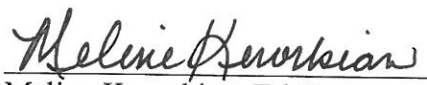
Dec 6, 2018
Date



James L. Parrish, Ph.D.
Dissertation Committee Member

12/6/2018
Date

Approved:



Meline Kevorkian, Ed.D.
Interim Dean, College of Engineering and Computing

12/6/2018
Date

College of Engineering and Computing
Nova Southeastern University

2018

An Abstract of an Idea Paper Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Development and Validation of a Proof-of-Concept Prototype for Analytics-based Malicious Cybersecurity Insider Threat in a Real-Time Identification System

by
Angel Hueca
November 2018

Insider threat has continued to be one of the most difficult cybersecurity threat vectors detectable by contemporary technologies. Most organizations apply standard technology-based practices to detect unusual network activity. While there have been significant advances in intrusion detection systems (IDS) as well as security incident and event management solutions (SIEM), these technologies fail to take into consideration the human aspects of personality and emotion in computer use and network activity, since insider threats are human-initiated. External influencers impact how an end-user interacts with both colleagues and organizational resources. Taking into consideration external influencers, such as personality, changes in organizational policies and structure, along with unusual technical activity analysis, would be an improvement over contemporary detection tools used for identifying at-risk employees. This would allow upper management or other organizational units to intervene before a malicious cybersecurity insider threat event occurs, or mitigate it quickly, once initiated.

The main goal of this research study was to design, develop, and validate a proof-of-concept prototype for a malicious cybersecurity insider threat alerting system that will assist in the rapid detection and prediction of human-centric precursors to malicious cybersecurity insider threat activity. Disgruntled employees or end-users wishing to cause harm to the organization may do so by abusing the trust given to them in their access to available network and organizational resources. Reports on malicious insider threat actions indicated that insider threat attacks make up roughly 23% of all cybercrime incidents, resulting in \$2.9 trillion in employee fraud losses globally. The damage and negative impact that insider threats cause was reported to be higher than that of outsider or other types of cybercrime incidents. Consequently, this study utilized weighted indicators to measure and correlate simulated user activity to possible precursors to malicious cybersecurity insider threat attacks. This study consisted of a mixed method approach utilizing an expert panel, developmental research, and quantitative data analysis using the developed tool on simulated data set. To assure validity and reliability of the indicators, a panel of subject matter experts (SMEs) reviewed the indicators and indicator categorizations that were collected from prior literature following the Delphi technique. The SMEs' responses were incorporated into the development of a proof-of-concept prototype. Once the proof-of-concept prototype was completed and fully tested, an empirical simulation research study was conducted utilizing simulated user activity within a 16-month time frame. The results of the empirical simulation study were analyzed and presented. Recommendations resulting from the study also be provided.

Acknowledgements

I pay homage to my ancestors, on whose shoulders I stand, to do great things in life. I pay homage to my Ori for encouraging me to think big and expand my horizons. I pay homage to my Egbe, my community here on earth, and in heaven, that support me in all my endeavors. I pay homage to my Orisha, and Ifa, for their guidance and keeping me on the right path. I pay homage to Olodumare, and all the benevolent divinities in the universe for their unconditional love and support.

First and foremost, my dissertation committee chair, Dr. Levy. My deepest appreciation for your continued support, your infinite patience, and for believing in me and this project. This would not have been possible without you. Your knowledge and ability to make me think critically, have been invaluable on this journey. In addition, because of your support, I have had the opportunity to attend the International Institute of Applied Knowledge Management (IIAKM) conference in Europe, to present in Portugal, Slovenia, and Italy. At the conference I met many esteemed scholars, whose expertise and questions encouraged me view the research problem from different lenses and approaches. To my committee, Dr. Michelle Ramim, and Dr. James Parrish, I thank you also for your knowledge, encouragement and feedback to further strengthen this research. My research partner Karla Clarke, you were not only great to work with, but also became a great friend, thanks for your support! Dan Falk, my statistics and SAS guru, thank you for all your help. The big data wrangling and statistical analysis could not have been completed without your assistance.

The doctoral process and this dissertation have been one of the most intense undertakings I have ever done. I am fortunate to have had my family, and a group of people in my life who have supported this process. To all of you, thank you for your support and encouragement.

Last, but certainly not least, my husband Jonathan, you've been by my side through this entire journey. I am sincerely grateful for the support, encouragement, and patience, you provided on a daily basis. The sacrifices you made for me while I was completing this research, truly made it possible to move forward. Here's to free weekends!

Table of Contents

Abstract iii

Acknowledgements v

List of Tables vi

List of Figures viii

Chapters

1. Introduction 1

Background 1
Problem Statement 2
Dissertation Goal 4
Research Questions 8
Relevance and Significance 10
Barriers and Issues 11
Assumptions, Limitations, and Delimitations 12
Definition of Terms 15
Summary 18

2. Review of the Literature 20

Introduction 20
Cyber Threat Vectors 22
Major Types of Cyber Threats 23
Insider Threat 35
Incident Response 49
System Security Baseline Standards and Guidelines 54
Cybersecurity Monitoring 58
Delphi Technique 66
Data Mining 64
Data Modeling and Simulation 72
A Summary of What is Known and Unknown in Research Literature 80

3. Methodology 80

Overview of Research Design 81
Instrument Development 83
Reliability and Validity 120
Population and Sample 113
Proof-of-Concept Tool and Simulation 116
Resources 119
Summary 123

4. Results 125

Overview 125
Phase 1 - Expert Panel 126
Phases 2 and Phase 3 - Analysis of Simulated User Activity 135
Summary 148

5. Conclusions, Implications, Recommendations, and Summary

Conclusions 150

Implications	152
Recommendations and Future Research	153
Summary	154

Appendices

A. Institutional Review Board Approval Letter	158
B. Expert Recruitment Email	159
C. Expert Panel Survey Instrument - Delphi 1	Error! Bookmark not defined.
D. Expert Panel Suvery Instrument - Delphi 2	175

References

176

List of Tables

Tables

1. Summary of Impact of Cyber Threats 22
2. Summary of Major Types of Threats 24
3. Summary of External Attacks 26
4. Summary of Malware, Spyware, Worms, Bots, and Viruses 30
5. Summary of Social Engineering (Phishing, Vishing, & Impersonation) 32
6. Summary of Malicious Insiders 36
7. Summary of Observable Behavior 39
8. Summary of Insiders as Adversaries and Cyber Adversarial Thinking 40
9. Summary of Insider Threat Cases Overview 42
10. Auditable Attributable Events or Activities 44
11. Summary of Cyber Threat Indicators and Categories 47
12. Summary of Incident Response 52
13. Summary of Intrusion Detection and Prevention Systems (IDPS) 52
14. Summary of Security Information and Event Management (SIEM) Solution 54
15. Summary of Aim and Scope of a Security Policy 56
16. Technical Cybersecurity Indicators 59
17. Summary of Insider Technical Event Indicators 58
18. Human-centric Indicators – Five Factor Model of Personality (FFM) 60
19. Summary of Insider Personality and Human-Centric Indicators 61
20. Summary of Delphi Technique 67
21. Summary of Data Mining 67
22. Summary of Pattern Recognition 71

23. Summary of Trend Analysis	71
24. Summary of Data Modeling and Simulation	73
25. Summary of Cross-Validation, the Bootstrap, and the Jackknife	75
26. Indicators Used in Phase 1 Tentative Survey Instrument	87
27. Correlation Coefficient Interpretation	105
28. Risky Key Word Dictionary	
29. Summary of Research Question Triangulation	118
30. Frequency Table for SME Demographics	128
31. Means and Standard Deviations of Importance of Indicators	130
32. Means and Standard Deviations of Importance of Indicator Categories	132
33. Means and Standard Deviations of Importance of Indicator Weights	133
34. SME Identified Correlations	135
35. Decoy File Indicators	137
36. Crosstabulation Between System-Identified Indicator Activity and Malicious User	139
37. Crosstabulation Between SME-Identified Indicator Activity and Malicious User	141
38. Results of Bivariate Binary Logistic Regression with System-Identified Indicators Predicting Likelihood of Malicious User	143
39. Results of Bivariate Logistic Regression with SME-Identified Indicators Predicting Likelihood of Malicious User	143
40. Multivariate Binary Logistic Regression with Indicators Predicting Likelihood of Malicious User	145
41. Indicator SME-Identified Average Importance, OR, and Significance of Indicators	147

List of Figures

Figures

1. AI-InCyThR Proof-of-Concept Prototype Model 6
2. Incident Response Life Cycle 49
3. Overview of the Research Design Process 82
4. Proposed Indicator Correlation Matrix 96

Chapter 1

Introduction

Background

As society relies increasingly on information systems (IS), the threat of malicious insider activity continues to be of paramount concern in both the public and private sectors (Glasser & Lindauer, 2013). Recognizing insider threats has presented one of the most complex challenges in the information security field with even the definition of “insider threat” proving difficult (Costa et al., 2014). Due to the nature of the insider threat domain, malicious insiders can be expected to attempt to hide their actions utilizing techniques believed to evade detection, usually until their desired objective has been achieved (Young, Memory, Goldberg, & Senator, 2014). Schultz (2002) defined an insider attack as “the intentional misuse of computer systems by users who are authorized to access those systems and networks” (p. 526). Moreover, in numerous insider attacks, management and co-workers observed that offenders had exhibited signs of stress, disgruntlement, or had other issues, yet no one raised an alarm (Greitzer, Kangas, Noonan, & Dalton, 2010). This research aimed at developing a simulated, data-driven, proof-of-concept prototype that would assist in the evaluation and prediction of malicious insider threat activity. This was necessary because, as noted by Greitzer, Kangas, Noonan, Brown, and Ferryman (2014), if these human-centric as well as psychosocial precursors are evaluated properly and in a timely manner, they could alert an organization about a developing insider attack.

The remainder of this draft is organized as follows. First, a statement of the specific research problem this research study will address is presented. Second, the main

dissertation goal, research questions, as well the relevance and significance of this research will be discussed. In Chapter 2 a brief literature review of related research is presented regarding each of the relevant areas: cyber threat vectors, insider threat, incident response, system security baseline standards and guidelines, cybersecurity monitoring, as well as, data mining, data modeling, and simulation. Next, specific barriers and limitations will be discussed. Chapter 3 presents the methodology for this research study and will outline the specific data analysis that will be used to formulate user and indicator linear models. Furthermore, Chapter 3 will outline simulated model development, as well as, the specific model development steps.

Problem Statement

The research problem this study addressed was the imminent challenge to mitigating cybersecurity insider threats from employees or contractors who may bring harm to the organization by misusing information systems, computer networks, or data (Sood, Zeadally, Member, & Bansal, 2015). The threat posed by insiders to organizations and government agencies has continued to be of serious concern because it can expose the establishment and their sensitive information (Nurse et al., 2014). Nostro, Ceccarelli, Bondavalli, and Brancati (2014) stated that it is particularly challenging to identify insiders and the possible threats they pose to an information system. This is primarily due to the nature of the attackers, who are often company employees (or employees of an authorized contractor) motivated by social and economic gains. According to Lindauer, Glasser, Rosen, and Wallnau (2013), malicious acts carried out by these trusted insiders include, but are not limited to, theft of intellectual property or national security

information, fraud, and sabotage. Additionally, within certain critical infrastructures, such as power grids, communication networks, and transportation services, insider threats are even more dangerous because they potentially threaten human lives and national security (Punithavathani, Sujatha, & Jain, 2015). According to Cummings, Lewellen, McIntire, Moore, and Trzeciak (2012), insiders they studied needed very little technical sophistication because they tended to exploit known or newly discovered design flaws. Cummings et al. (2012) noted that malicious activity was planned in advance, with organizations suffering financial losses ranging from hundreds, to hundreds of millions of dollars; these malicious acts were committed during working hours. Almeahmadi and El-khatib (2014) stated that “insiders are the trusted, authorized entities in an organization who are assigned privileges and know how to navigate through a facility or system and access valuable materials easily, compared to unauthorized entities” (p. 1). Insider threats commonly act by exploiting their own user accounts to the capacity of their assigned privileges and access rights, while abusing their job functions (Fuchs & Gunter, 2010).

At the time of this study, insider threat responses, being largely reactive, attempted to identify malicious behavior after an event has occurred, therefore, it lacked a predictive analytic methodology (Greitzer, Frincke, & Zabriskie, 2010). According to Greitzer and Hohimer (2011), insider threats are manifested within socio-technical systems, which combine “social, behavioral, and technical factors that interact in complex ways” (p. 30). According to Greitzer et al. (2009), observations of user behavior are processed from cyber and psychosocial data that infer indicators, including excessive access attempts, the presence of automated scripts, registry entries, IDS/IPS events, and firewall logs. For the purposes of this study, these observations are referred to as “input

indicators.” By analyzing input indicators and their relationships in a timely manner, organizations can be alerted of a developing cyber-attack (Greitzer et al., 2010).

Where no rational relationships to employee activities exist in security event and information management (SEIM) solutions, tools that monitor psychological indicators, can help identify employees who exhibit elevated insider threat risk, allowing the organization to provide assistance to these employees before these situations escalate (Greitzer et al., 2014). These employee activities and additional input indicators can be matched with physical security inputs to provide a more robust predictive platform. Moreover, according to Greitzer et al. (2009), “a benefit of a predictive approach is the potential for an attentive manager to speak with stressed employees and possibly avert a cyber incident by addressing underlying problems” (p. 4). Additionally, it has been observed that in many insider cyber-attacks, supervisors and co-workers recognized that suspects displayed signs of stress or disgruntlement, yet raised no alarms with senior management or human resources personnel (Greitzer, Dalton, Kangas, Noonan, & Hohimer, 2012). Warkentin and Willison (2009) acknowledged that the insider threat has been repeatedly called the greatest threat to information security, yet is often overlooked by organizations and the intelligence community, which focus primarily on protecting the network perimeter from external threats.

Dissertation Goal

The main goal of this research study was to design, develop, and validate a proof-of-concept prototype for a malicious cybersecurity insider threat alerting system that would assist in the detection and prediction of malicious insider threat activity using human-centric technical activities as well as individual employee psychometric rating

scales. A prototype is defined as an original model on which something is patterned (Levy, 2007). Figure 1 depicts an outline and initial design of the proposed Analytics-based Identifying Insider Cybersecurity Threat in Real-time (AI-InCyThR) system. The AI-InCyThR system would assist in identifying behaviors, activities, and other inputs as identified by the expert panel, in an effort to identify at-risk employees and alerting of a possible cyber-attack before it has materialized.

The need for this work has been demonstrated by the work of Bishop and Carrie (2008), Greitzer et al. (2008, 2009, 2010, & 2012), Greitzer and Hohimer (2011), Lawton (2008), as well as Magklaras and Furnell (2002). Greitzer et al. (2012) outlined that identifying the warning signs of insider threats ahead of a full-blown cyber-attack requires the communication and coordination of several factors. These include assessing the capabilities, opportunities, and motivations of an end-user, or the organizational ability to evaluate risk levels for employees. In addition, Schultz (2002) suggested that personality factors, particularly introversion, can be used in predicting insider attacks.

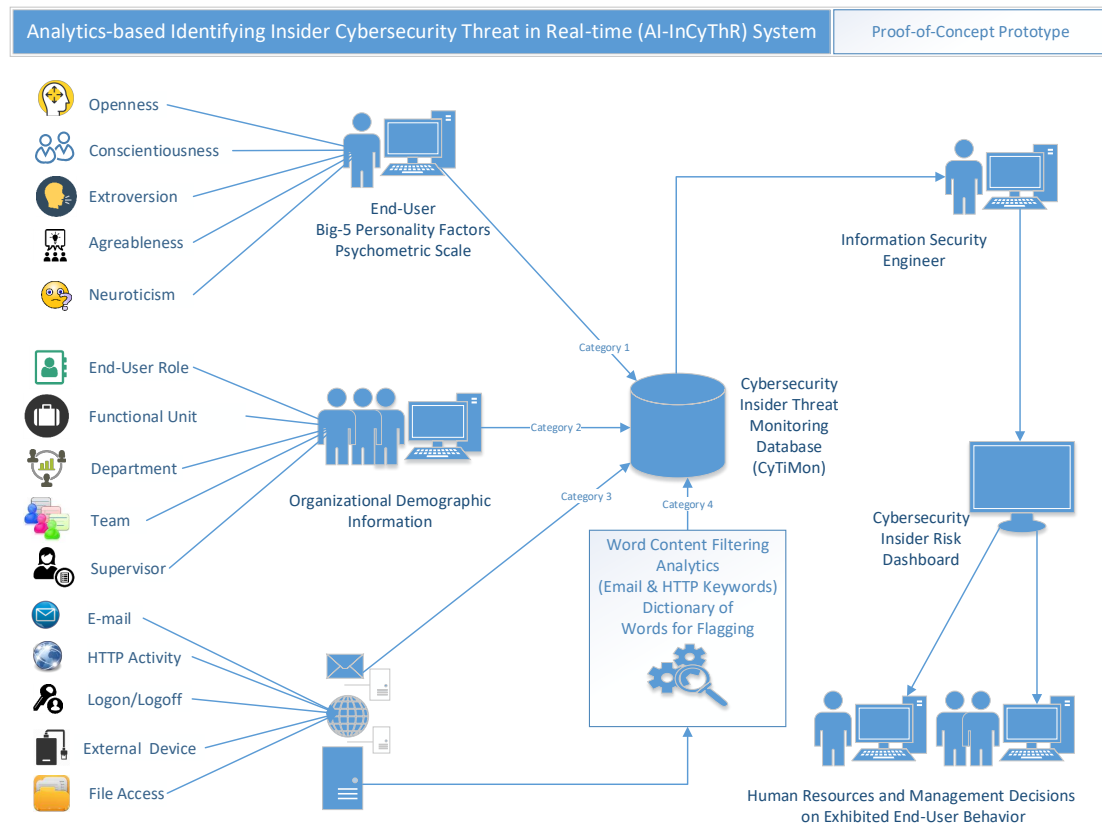


Figure 1. AI-InCyThR Proof-of-Concept Prototype Model

Greitzer and Hohimer (2011) defined several technological sources representative of host/network cyber data to be monitored for insider threat analysis, which were integrated with psychometric indicators as presented by Greitzer et al. (2009). The AI-InCyThR system aimed to address the problem of insider threat by focusing on both technical as well as behavioral aspects (Greitzer et al., 2008).

Figure 1 depicts the AI-InCyThR proof-of-concept prototype. The proof-of-concept prototype developed in this study will analyze indicators from two categories, those being the Five Factor Model (FFM) of personality, and collected simulated data sources / network resources. The categories can be further delineated into specific

personality factors, user behavior, and electronic sources. Indicators aggregation and analysis occurred using the Cybersecurity Threat-Insider Monitoring Database (CyTiMon). Analyzed and processed data were reviewed by an information security professional through data visualization for correctness, while providing a real-time assessment of the network heartbeat for alerting management of unusually suspicious combination of indicators occurs.

This study aimed to specifically align with Department of Defense (DoD) Directive Number 5205.16; The DoD Insider Threat Program:

This directive ...Establishes policy and assigns responsibilities within DoD to develop and maintain an insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate actions by malicious insiders who represent a threat to national security or DoD personnel, facilities, operations, and resources. (Department of Defense, 2014, p. 1)

This study built on the work of Greitzer et al. (2012) and intended to develop as well as validate an indicator instrument for the assessment of behaviors and technical actions related to the potential risk of cybersecurity insider threats. This research aimed to acquire improved data on the relative distribution, interrelationships, and weight (i.e. level of importance), with respect to cybersecurity insider threat risks of concerning behaviors and personal predispositions as noted by Band et al. (2006).

The seven specific goals of this research study are as follows. The first specific goal of this study was to identify a set of cybersecurity input indicators as pinpointed by subject matter experts (SMEs), which can help in the identification of precursors to malicious cybersecurity insider threat activity. The second specific goal of this study was

to develop a set of cybersecurity events that can be categorized and linked to the SME-identified set of cybersecurity input indicators. The third specific goal of this study was to identify expert-approved weights (i.e. level of importance) for the SME-identified cybersecurity input indicators. The fourth specific goal of this study was to establish the expert identified most significant correlations between cybersecurity input indicators. The fifth specific goal of this research was to determine which of the identified cybersecurity input indicators display a high rate of false positives or false negatives. The sixth specific goal of this research was to recognize which of the simulated user activity indicators were identified by the AI-InCyThR proof-of-concept prototype as significant input indicators to identify insider threat activity. Therefore, the seventh specific goal this research was to establish which simulated user activity correlations were identified by the SME's different that those identified by the AI-InCyThR proof-of-concept prototype as significant to identify insider threat activity.

Research Questions

The main research question this study addressed was: What human-centric technical activity and psychometric indicators are precursors to malicious end-user activity, making those activities rise above a certain threshold to be identified as potential insider threats? The specific research questions (RQ) this study addressed, as seen in Figure 2, were:

RQ1: What are the important cybersecurity indicators validated by the expert panel that can assist in the detection of insider threat activity?

RQ2: What are the expert-validated cybersecurity indicator categories?

RQ3: What are the expert-approved weights for the identified cybersecurity indicators?

RQ4: What are the expert-identified most significant correlations between cybersecurity indicators?

RQ5a: What cybersecurity indicators were identified in experimental settings to have a high rate of false positives as measured by the AI-InCyThR prototype?

RQ5b: What cybersecurity indicators were identified in experimental settings to have a high rate of false negatives as measured by the AI-InCyThR prototype?

RQ6: What simulated user activity *indicators* were identified by the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity?

RQ7: How are the simulated user activity correlations that were identified by the SMEs different than those identified by the AI-InCyThR proof-of-concept prototype as significant to identify insider threat activity?

Relevance and Significance

Relevance

This research study was relevant as it sought to gain a better understanding of how additional categorized cybersecurity indicators can assist in identifying potential malicious activity and motivating circumstances. Precise identification of malicious

activity can significantly affect the accuracy and validity of a SIEM solution, assisting in the mitigation of an insider threat incident through real-time alerts and visualization. This is supported in the literature on a study conducted by Greitzer et al. (2012), who determined that a model of insider threat risk can be developed to produce predictions that are highly correlated with expert judgments (p. 2400). This research is also supported by the work of Hashem, Takabi, Ghasemigol, and Dantu (2016), who demonstrated that it is “almost impossible to stop the insider threat attack at the gate” (p. 33), as well as, that a user-centric monitoring and detection framework is needed for the early detection of malicious insider threat activity. According to Bishop, Nance, and Claycomb (2017), “analyzing and detecting insider threats involve both technical and non-technical approaches across many different disciplines, including human-oriented ones” (p. 2637), this research aimed at analyzing both technical and psychometric indicators for the detection of potential malicious cybersecurity insider threat attacks. Various case studies using human-centric indicators must be considered to measure precursors to insider threat activity; specifically, in an environment where some tasks may be performed manually, while other may be computer based (Greitzer et al., 2012; Gritzalis, Stavrou, Kandias, & Stergiopoulos, 2014).

Significance

This research study was significant in that it advanced contemporary research in insider threat detection, as well as, facilitate an increase in the cybersecurity body of knowledge. In regard to how SIEM solutions integrate human-centric input feeds with technical input feeds, this study identified employee technical activity correlations, coupled with the employees psychometric rating, to assist in the detection of an insider

threat attack. As noted by Hazari, Hargrave, and Clenney (2008), there is a human element to information security that deals with psychology, motivation, education, and social aspects. According to West (2008), “understanding these principles on how users come to make decisions about security may suggest places where we can improve the outcome of the decisions” (p. 36). This research was significant in that it contributed to fulfilling the need for a more thorough validation of insider threat models and tools as expressed by Greitzer et al. (2010). Additionally, this research contributes to combating insider threats through the development of methods and models for analyzing suspicious computer activities that may predict insider attacks (Greitzer et al., 2010).

Barriers and Issues

One potential barrier for this research study was obtaining the permission necessary to survey cybersecurity industry experts for determining input indicators. Institutional Review Board (IRB) approval is required to survey study participants. Approval was obtained in advance to conduct the study with input from industry experts. This study required a minimum of 15 SMEs per round of data collection. Therefore, to minimize the feasibility of a low response rate, 336 SMEs were contacted for both Delphi 1 and Delphi 2, during Phase 1 of this research study.

The use of simulated data was another potential barrier. While simulated data gives researchers greater control over the simulation environment, Hill and Malone (2004) explained that the use of simulated data can have significant effects on the results. According to them, “models that are either too clean and well behaved or are unrealistic with respect to error and other real-world characteristics can provide misleading results”

(Hill & Malone, 2004, p. 972). This was mitigated by the use of benchmarking from similar studies, which provided a point of reference in the data analysis (Hill & Malone 2004; Sekeran, 2003).

Another issue that may have arisen was model validity. Validation has to do with determining whether or not a simulation model is an acceptable and accurate representation of reality (Giannasi, Lovett, & Godwin, 2001). According to Martis (2006), when working with simulation models, some things to consider include: 1) a model should be assessed for its usefulness, rather than its absolute validity 2) if a model cannot have absolute validity, however, it should be valid for purposes for which it was intended; and 3) as a model passes its various test assurances, validity in that model is heightened. As a result, using the proof-of-concept prototype, a series of tests performed on the simulation data compared with benchmarks outlined in similar studies and literature, progressed this study towards successful research level design and development.

Assumptions, Limitations, and Delimitations

Assumptions

1. It was assumed that cybersecurity SMEs were ethical and honest in their responses.
2. It was assumed that a significant majority of the cybersecurity SMEs would have participated in all three phases of SME-required data collection.
3. It was assumed that the simulated user activity data set was sufficient for the necessary analysis and indicator correlation exercises.

Limitations

Since the Delphi technique is a multi-round study, much time is required, so some participants will, inevitably, not continue with the Delphi process, complicating data collection (Gordon, 2009). This may have served as a limitation. As an incentive for continued participation, Scheele (1975) suggested that researchers consider “in kind” gifts for participation, which the study sponsor can provide at moderate cost. According to Ellis and Levy (2010), another possible limitation is the expert opinions collected during the Delphi technique process, since these opinions are limited to the members recruited. To elaborate further, as explained by Linstone and Turoff (2002), expert opinions are “nearly always unconsciously biased” (p. 567). In order to mitigate this limitation, it was ensured that there was representation from all relevant groups within the specific field for the expert panel (Linstone & Turoff, 2002). Another potential limitation of this research study was assuring that the study remained within its accepted parameters and scope.

Developmental research is distinguished from product development by a focus on complex, innovative solutions that have few, if any, accepted design and development principles; a comprehensive grounding in the literature and theory; empirical testing of a product’s practicality and effectiveness; as well as, thorough documentation, analysis, along with reflection on processes and outcomes. (Ellis & Levy, 2009, p. 328)

As noted by Ellis and Levy (2008), while the research problem serves as the starting point, the literature review serves as the foundation from which the research is built. Incorporating the findings from the literature review, with expert panel

recommendations elicited through the Delphi technique, progressed this study towards a successful research level design and development effort.

Measuring the AI-InCyThR proof-of-concept prototype analysis against simulated data may have been another possible limitation. Due to the nature of the simulated data, the rate of false positives and false negatives may threaten the validity and reliability of any malicious cybersecurity insider threat precursors detected. To mitigate this limitation, a longitudinal baseline was created where simulated user activities were broadcast over a period of time, and predictions of the model were compared to simulated observed events (Greitzer et al., 2012). Additionally, a continuous review of the data recorded along with its respective scoring and weighting ensured that participants' responses as well as indicator weight assignments were correctly applied prior to conducting the empirical study.

Delimitations

A possible delimitation of this study is that it was limited to a single set of simulated data. Moreover, that many study's Delphi participants were limited to a single, higher education institution. The responses of the participants may be a delimitation of the study, as institutional culture may have affected how participants answer questions and weigh activity indicators.

Definition of Terms

The following represents terms and definitions.

Biclustering – “a popular technique, which allows simultaneous clustering of the rows and columns of a matrix” (Reddy & Aziz, 2010, p. 4)

Correlation Clustering – “a special type of clustering which defines the similarity between objects in terms of correlation between features, that is, it is a clustering approach which assigns two data points to the same cluster” (Reddy & Aziz, 2010, p. 4)

Correlation Coefficient – a type of statistical measure that indicates the magnitude of relationship between two variables, while also showing how the two variables interact with each other (Ambusaidi et al., 2014)

Data Matrix – “an organization of raw scores or data, where the rows represent subjects, or cases, and columns represent variables” (Mertler & Vanetta, 2010, p. 3)

Data Mining – a process of discovering hidden patterns and information from the existing data, as well, cleaning the data so as to make it feasible for further processing (PhridviRaj & GuruRao, 2014)

Data Visualization – “the use of images to represent information” (Few, 2007, p. 2)

Delphi – “a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem” (Okoli & Pawlowski, 2004, p. 16)

Holt-Winter Method – a method which allows data to be modeled by a local mean, a local trend and a local seasonal factor which are all updated by exponential smoothing (Chatfield & Yar, 1988)

Incident Response – “is the reaction to an identified occurrence whereby responders classify an incident, (then) investigate and contain the incident” (Brennan & Jolo, 2015, p. 2)

Indicators – documented employee behaviors, intellectual property, employee activity on networks, information on organizational property networks, and information technology (IT) architecture (Costa et al., 2014, p. 1)

Information Security Event – the identified occurrence of a system, service, or network state indicating a possible breach of information security, policy or failure or controls, or a previously unknown situation that may be security relevant (International Standards Organization, 2011)

Information Security Incident – a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening security (International Standards Organization, 2011)

Information Visualization – the transformation of data into a visual representation, so that users can better understand the data (Brunetti, Auer, García, Klímek, & Nečaský, 2013)

Insider Threat – “a trusted entity that is given the power to violate one or more rules in a given security policy... the insider threat occurs when a trusted entity abuses that power” (Bishop, 2005, p. 1)

Malicious Insider Threat – “a current or former employee, contractor, or business partner who meets the following criteria: has or had authorized access to an organization’s network, system, or data; has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems” (Silowash et al., 2012, p. 2)

Motivation – the key influencers on behavior though other options are available (Tolman, 1938)

Multivariate data – “consists of more than one dimension/variable, where each axis represents a variable of the data set. The N-axis are drawn as vertical lines with equal spacing, and each data element displayed as is a series of connected points along the dimensions” (Steinparz, Abmair, Bauer, & Feiner, 2010, p. 2).

Mutual Information – a generalized correlation analogous to a linear correlation coefficient, but sensitive to any relationship, including nonlinear correlations (Roulston, 1999)

Nonlinear Correlation Coefficient – “a method based on mutual information, which is a quantity measuring the relationship between two discrete random variables” (Ambusaidi et al., 2014, p. 80)

Pearson’s Correlation Coefficient – “one of the basic linear correlation methods used to measure dependence between two variables” (Ambusaidi et al., 2014, p. 79)

Precursor – “an activity that, when observed, flags the associated user as a potential malicious insider. Each precursor can be assigned a score, which reflects the extent to which the precursor identifies classifies someone as a malicious insider” (Marty, 2008, p. 393).

Proper Linear Model – “one in which the weights given to the predictor variables are chosen in such a way as to optimize the relationship between the prediction and the criterion” (Dawes, 1979, p. 571)

Principle Curves – “nonlinear summarizations of multidimensional data points represented by a smooth, one-dimensional curve” (Reddy & Aziz, 2010, p. 4)

Risk Based IT Auditing – an institution’s ability to report and detect important risk factors in an approach that focuses on the response of the organization to the risks it faces in achieving its goals and objectives (Lovaas, 2009, p. 485)

Synthetic Data – “data that are generated by simulated users in a simulated system, performing simulated actions; simulations may involve human actions to some extent or be an entirely automated process” (Barse, Kvarnstrom, & Johnson, 2003, p. 2)

Summary

The research problem that this study addressed was the imminent challenge to mitigate cybersecurity insider threats from employees or contractors who may pose harm to the organization by misusing the information systems, computer networks, or data (Sood et al., 2015). To address this research problem, this study has set a main goal to design, develop, and validate, using SMEs, a proof-of-concept prototype for a malicious cybersecurity insider threat alerting system that would assist in the detection and prediction of malicious insider threat activity. For the purposes of this study, the SMEs were not the end-users of the prototype. The SMEs who participated in this study were validating both the technical and psychometric input indicators required for the detection of precursors to malicious cybersecurity insider threat activity.

This developmental research study was conducted in three phases of data collection and analysis. During Phase 1, this developmental study conducted Delphi method data collection from SMEs to validate, as well as, assign, weights to technical activity and psychometric cybersecurity indicators for measuring malicious cybersecurity insider threat activity, as identified in the literature and NIST Special Publications. Thus, in Phase 2, this developmental study added the aforementioned developed and validated

technical activity and psychometric indicators into the AI-InCyThR proof-of-concept prototype that was used to collect the simulated user activity data, refine the data identifying false positives and negatives, as well as, measure indicators, indicator correlations, and indicator weights on over several million simulated user activity logs, representing a span of over a year and a half of the simulated user activity on a private network. Therefore, in Phase 3 of this developmental study, an analysis was performed of the collected evidence and indicator relationships against a previously identified Minimum Security Baseline (MSB), as well as, establish an over detection of accuracy of predicted malicious cybersecurity events. Subsequently, a conclusive report with conclusions and recommendations was produced.

Chapter 2

Review of the Literature

Introduction

To lay the theoretical foundation for this developmental research study, this chapter will provide a synopsis of the literature relevant to not only malicious cybersecurity insider threats, but also to data simulation considerations, high-level technical and psychosocial indicators, as well as, cyber threats. As noted by Pare, Trudel, Jaana, and Kitsiou (2015), “the literature review section helps the researcher understand the existing body of knowledge and provides a theoretical foundation for the proposed empirical study” (p. 183). Moreover, an effective literature review assists the researcher in identifying where new research is needed, as well as, justifies the study as one that contributes something new to the body of knowledge (Levy & Ellis, 2006).

To ensure breadth, depth, and rigor in this study, a search of the Information Systems (IS) literature domain was conducted using several databases of interdisciplinary fields, including IS, business, and psychology. This literature review process revealed existing cybersecurity knowledge, technical, as well as, psychosocial indicators, and research gaps, along with the theoretical foundations for this research study of validating, developing, as well as empirically testing technical and psychosocial indicators as precursors to malicious cybersecurity insider threats. Furthermore, information on exercising the expert methodology is presented.

Cyber Threat Vectors

Impact of Cyber Threats

As reported by IBM Security (2016), in taking a holistic view of targeted industries, “it is clear that virtually no industry was immune to the exploits of today’s attackers” (p. 3). Most organizations are well aware of the dangers posed by cyber attacks; however, to date, the Federal Government has no well-developed, nor publicly known strategy for deterring these types of attacks (Kugler, 2009). Should attackers disrupt or destroy infrastructures – such as the energy grid, clean drinking water supply, communications, and public transportation – on which society heavily relies, the residual effects on the health and safety of citizens may be severe (Luijff, 2012). As clarified by Luijff (2012), these frameworks are considered Critical Infrastructures (CI) and their undisturbed functioning is highly dependent on the security of their underlying support systems, such as information assets, as well as, internal and external communication links. As suggested by Awan, Burnap, and Rana (2016), because of the sophistication of new and evolving attacks, network-level defenses alone do not suffice as an overall information security plan. Governments, organizations, and individuals may very easily become the victims of cyber crimes as well as, becoming unknowing assistants to cyber criminals (Awan et al., 2016), thus, contributing even more to the insider threat phenomenon.

Relating to existing cybersecurity terminology, Verizon (2016) identified an incident as “a security event that compromises the integrity, confidentiality, or availability of an information asset” (p. 5). Similarly, Verizon (2016) identified a breach as “an incident that results in the confirmed disclosure (not just potential exposure) of

data to an unauthorized party” (p. 5). While there are many different types of cyber attacks and adversaries, the 2016 Verizon Data Breach Investigations Report (VDBIR) issued by Verizon identified “nine reoccurring combinations of the, who (actors), what (assets), how (actions), and why (motives) among other incident characteristics” (p. 22), not including miscellaneous errors. The items in these reoccurring combinations are noted as 1) privilege misuse, 2) physical theft/loss, 3) denial of service, 4) everything else, 5) crimeware, 6) web application attacks, 7) POS intrusions/payment card skimmers, 8) cyberespionage, 9) miscellaneous errors.

Table 1

Literature Summary of Impact of Cyber Threats

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Awan et al., 2015	Empirical study	462,787 network traffic instances, 278 unique threats, 6 categories	Network analysis	Development of a risk assessment framework for managing network security risk
IBM Security, 2015	Empirical observations	8000 client devices, from 100 countries	Security awareness	Cyber strategy, prioritizing security objectives,
Kugler, 2009	Case study	Compilation of U.S. cybersecurity guidelines	Analytical methods and metrics used in decision making for cyber-attack deterrence	Ascertained the need for an extended cyber deterrence strategy for the U.S. and its allies

Table 1

Literature Summary of Impact of Cyber Threats (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Luijff, 2012	Literature review		Critical infrastructure information (CII)	Taxonomy of threats, attack actors, and motives in reference to CII
Verizon, 2016	Case study	100,000 incidents, of which 3,141, were confirmed data breaches	68 contributing organizations	9 attack vectors identified in 2014 remain prevalent in cyber-attacks, actions taken by an adversary are not exclusive to any single pattern

Major Types of Cyber Threats

According to Randazzo, Keeney, Kowalski, Cappelli, and Moore (2005), statistics vary on the frequency of cyber attacks carried out by insiders, compared with those cyber attacks carried out by actors external to the target organization. To defend against external cyber attacks, organizations can implement physical and technical security measures, such as firewalls, intrusion detection systems (IDS), and authentication mechanisms (Andersen et al., 2004). As noted by Carlin (2016), “knowing which specific computer or network caused the malicious activity doesn’t necessarily tell you which person or organization ordered, carried out, or supported the hack” (p. 387). This study followed the example of Greitzer et al. (2009) in developing a proof-of-concept prototype that utilizes a predictive modeling approach by analyzing psychosocial and cyber indicators. Accurately identified cyber indicators can be utilized to correctly assess not

only cyber activity on a network, but also an employee's behavior and possible malicious actions.

Table 2

Literature Summary of Major Types of Cyber Threats

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Anderson et al., 2004	Case study	Six insider threat cases	Cybersecurity insider threat detection	Systemic approach to cybersecurity: policies and procedures to mitigate insider threat attack
Carlin, 2016	Conceptual paper	U.S. federal cybersecurity guidelines	Cyber-attack deterrence	Presented a whole-of-government approach to cyber threats
Randazzo et al., 2005	Aggregated case-study analysis	23 incidents carried out by 26 insiders in the banking and financial sector	Cybersecurity insider threat detection	Information development of commonalities within the cases studied

External Attacks

Christ (2007) illustrated how computer based cyber attacks have evolved over time, where network-based attacks have been replaced by more sophisticated Web applications or by externally based attacks. One of the most common external attacks floods a target system with data requests, overloading the resource and rendering it inaccessible, this is known as a Denial of Service (DoS) (Meyers, Powers, & Faissol,

2009). The DoS attack is intended to compromise the availability of networks and systems, to include both network resources and applications (Verizon, 2016). By overwhelming a system, the DoS attack degrades service or causes a complete service interruption. However, Werlinger, Muldner, Hawkey, and Beznosov (2010) mentioned that diagnosing a DoS was undemanding because it could be achieved by the inspection of specific network activity, since DoS is sending the same data packets or requests over and over again. In comparison, a Distributed Denial of Service (DDoS) “is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems” (Specht & Lee, 2004, p. 543). According to Carlin (2016), in March of 2016, the U.S. Government had identified and publicly charged a group of Iranian hackers with carrying out a DDoS directed at the U.S. financial sector, which affected 46 financial institutions over the course of 176 days. The attack disrupted the financial institutions’ online services for hundreds of thousands of Americans, who in turn were unable to process any online banking transactions (Carlin, 2016).

Other Web-based attacks include the SQL injection (SQLi), where the vulnerability in lack of input validation allows malicious actors to issue SQL commands via the Web application interface or Website, to issue illicit commands to the database (IBM Security, 2016; Verizon, 2016). According to Symantec’s 2016 Internet Security Threat Report, at the time of this study, Website owners were still not patching or updating their servers accordingly, leaving vulnerabilities for malicious actors to exploit (Symantec, 2016). The report also indicated that more than three-quarters of the Websites scanned had unpatched vulnerabilities, where one in seven, or 15%, were categorized as

“critical” in 2015 (Symantec, 2016). These Web-based and external vulnerabilities allow for a host of other threats to impact an organization’s information systems assets.

Table 3

Literature Summary of External Attacks

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Carlin, 2016	Literature review and synthesis		Cybersecurity threats and vulnerabilities	Development a strategy to disrupt national cyber threats
Christ, 2016	Conceptual paper		Web-based attack mitigation	Defense-in-depth approach using technology and user awareness
IBM Security, 2016	Case study	Compilation of 8000 client devices in over 100 countries	Cybersecurity threats and vulnerabilities	Prioritization of business objectives and risk tolerance needed to face cyber risks
Myers et al., 2009	Literature review and synthesis		Cyber threats and vulnerabilities	Taxonomy of cyber adversaries, corresponding methods, and skill level

Table 3

Literature Summary of External Attacks (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
--------------	--------------------	---------------	--------------------------------	-------------------------------------

Specht & Lee, 2004	Literature review and synthesis		DDoS attacks	Taxonomies to characterize the scope of DDoS attacks
Symantec, 2016	Case study	74,180 vulnerabilities, from 23,908 vendors, and 71,470 products	Cyber threats	Provided a series of best practice guidelines for consumers
Verizon, 2016	Case study	Culmination of Fortune 500 companies	Cyber breaches	Introduced Vocabulary for Event Recording and Incident Sharing (VERIS) framework
Werlinger et al., 2010	Empirical study	16 participant organizations	Cybersecurity incident response and mitigation	Illustrated the importance of the preparation, detection, and analysis phases participation

Malware, Spyware, Worms, Bots, and Viruses

Malicious software, known as *malware*, “has consistently been ranked as one of the key cyber threats to businesses, governments, and individuals” (Choo, 2011, p. 721). By definition, the term *malware* describes a classification of malicious code which changes the behavior of the operating system kernel, without user consent and in such a way that those changes cannot be detected without using the documentation feature of the operating system or other security applications (Rutkowska, 2006). Choo (2011) explained that malware can be categorized into two classifications, generic malware

intended toward the general public, and malware that has been coded for information stealing, pointed at specific organizations.

According to Meyers et al. (2009), a computer *virus* is a malicious program that has the ability to copy itself without the knowledge of the end-user. As Meyers et al. (2009) explained, “viruses are transferred when their host is connected with the target system, either via a computer network, the Internet, or a form of removable media” (p. 14). Similarly, a *worm* is described as autonomous malicious code that has the ability to propagate on its own, contains different payloads, and has no need to attach itself to existing files or programs (HPE Security Research, 2016; Meyers et al., 2009).

In comparison, a *bot*, originating from the word “robot,” is a specific application that can perform certain tasks faster than humans can; when many bots are dispersed to several computers across the Internet and connect with each other, they form a *botnet* (Eslahi, Salleh, & Anuar, 2013). The term *botnet* is used to describe a framework of hosts infected with malicious code “that are under the control of a human operator commonly known as the *botmaster*” (Abu Rajab, Zarfoss, Monroe, & Terzis, 2006, p. 1). In regards to botnets as global threats, Pilling (2013) illustrated how Cutwail, one of the largest botnets, is used to impersonate very well-known online retailers, mobile service providers, social networking sites (SNS), and financial institutions (p. 14). According to Pilling (2013), Cutwail is one of the primary methods for the deployment of malware downloaders, with anywhere from “175,000 to 500,000 active bots on any given day” (Pilling, 2013, p. 14). Pilling (2013) further elaborated on Cutwail’s popularity being due to malicious actors with easy access to Cutwail’s spam-as-a-service infrastructure.

Table 4

Literature Summary of Malware, Spyware, Worms, Bots, and Viruses

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Abu Rajab et al., 2006	Empirical study and longitudinal tracking of IRC botnets	3-month examination of 800,000 DNS domains	Malicious botnet infection	Botnets are an overall contributor to unwanted traffic on the Internet
Choo, 2011	Theoretical		Cyber threat landscape	Applied routine activity theory can be implemented to reduce the opportunities for cyber crime
Eslahi, 2013	Literature review and synthesis		Cybersecurity threat protection	Overview of botnet characteristics as well as, their malicious activities
HPE Security Research, 2016	Case study	Data collected by HPE Security, open source intelligence, ReversingLabs, and Sonatype	Cyber threat landscape	Overview of threat landscape encompassing several types of attacks as well as, legislative burdening on mitigation and research

Table 4

Literature Summary of Malware, Spyware, Worms, Bots, and Viruses (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
--------------	--------------------	---------------	--------------------------------	-------------------------------------

Meyers, 2009	Literature review and analysis	Cyber adversaries and attacks	Proposed cyber-adversary taxonomy
Pilling, 2013	Theoretical	Cybersecurity threat protection	Global cyber threats
Rutkowska, 2006	Literature review and analysis	Cyber adversaries and attacks	Proposed taxonomy to categorize stealth malware

Social Engineering (Phishing, Vishing, & Impersonation)

It has been well documented both in research and among organizations that their employees are the weakest link in information security (Bulgurcu, Cavusoglu, & Benbasat, 2010). Malicious actors exploit the weakness in end-users or employees by obtaining information from them under false pretenses and manipulation; this process is called *social engineering*. As reported by AT&T Security (2015), cybercriminals are becoming more sophisticated by exploiting an individual's information published on social media. This information can be used by malicious actors to appear to be the user's friend. As such, masquerading as a known and trusted person is an attempt to gain an employee's password or obtain other access through trickery or exploitation of the trusted relationship (Silowash et al., 2012).

Sood et al. (2015) explained how indirect attacks, such as social engineering, use other techniques like *phishing*, which “force users to visit the embedded links in phishing emails” (p. 8). In these type of social attacks, a victim is sent a spoofed email modeled after a real email, claiming to be from a coworker, bank, social network, or even an entity offering a “needed” software upgrade (Bowen, Devarajan, & Stolfo, 2011). Bowen et al.

(2011) elaborated on this technique, saying, “when the victim takes the bait, they are often greeted with some form of malicious software that attempts to install itself on the victim’s machine” (p. 2). According to Verizon (2016), “the main perpetrators for phishing attacks are organized crime syndicates and state-affiliated actors” (p. 18). The Verizon 2016 DBIR indicated that in 2015, there were 9,576 incidents reported, with 916 of these incidents confirming data disclosure. Verizon (2016) concluded that the main cause of these type of breaches is a failure of communication between the victim and the organizational staff, noting the need for much more effective communication between the victim and the IT staff.

Vishing, derived from “voice” and “phishing,” is where a “phone call is received with the attacker luring the receiver into providing personal information with the intention to cause harm” (Yeboah-Boateng & Amanor, 2014, p. 297). Due to the nature of telephony, the technology, be it land, mobile, or Internet Protocol (IP)-based, is susceptible to malicious vishing attacks, specifically because of its social and technological reach (Ollmann, 2007). Maggi (2010) emphasized that Voice over Internet Protocol (VoIP) is not a secure protocol, and illustrated how criminals can take advantage of these vulnerabilities by spoofing and impersonating call identifiers. Cyber attacks are carried out in a sophisticated manner, in which malicious actors use social engineering to bypass traditional two-factor authentication. In one such attack, as reported by Symantec (2016), malicious actors impersonated tax officials in an attempt to get individuals to download malicious email attachments. Malicious actors not only have the ability to impersonate outside entities, they also aim at assuming the identity of legitimate parties in a system, or by using trusted communication protocols. In the impersonation attack,

the adversary successfully assumes the identity of the target to carry out malicious activity (Adams, 2011). This research study focused on deliberate attacks, rather than accidental ones, and defined the malicious insider as noted by Cummings, Lewellen, McIntire, Moore, and Trzeciak (2012):

A current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. (p. vii)

This study took into consideration the concerns of Kugler (2009), Luijff (2012), and Awan et al. (2016) in creating a prototype that can be used to assist in the detection of malicious activities by those individuals with trusted access to organizational information resources.

Table 5

Literature Summary of Social Engineering (Phishing, Vishing, & Impersonation)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Adams, 2011	Literature review		Security literacy	Clarified the term "identification" within the cybersecurity scope
AT&T Security	Conceptual paper	Visibility into 10 petabytes of traffic daily	Social engineering	Identified phishing as a precursor to social engineering

Awan et al., 2016	Empirical study	462,787 instances representing threats over 144 hours	Computer network risk	Proposed a risk assessment framework that allows for high level view of network security
Bowen et al., 2011	Empirical study	500 phishing emails sent to 4,000 users	Social engineering	Identified that users can be trained using bogus phishing emails
Bulgurku et al., 2010	Empirical study	11 graduate students	Cybersecurity compliance	Demonstrated rationality based factors that drive employees to information security policy compliance
Cummings et al., 2012	Empirical study	Interviews with law enforcement and banking investigators involved in 80 insider fraud cases	Social engineering	Presented insider fraud models to establish countermeasures in. insider IT sabotage, insider theft of IP, and national security espionage

Table 5

Literature Summary of Social Engineering (Phishing, Vishing, & Impersonation) (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kugler, 2009	Conceptual paper		Cyber threat deterrence	Identified the need for a national cyber deterrence strategy

Maggi, 2010	Empirical study	PhonePhishing.info data set	Vishing (voice phishing)	Analysis of vishing reports submitted by victims
Ollman, 2007	Conceptual paper		Vishing (voice phishing)	Identified IP telephony and vishing as the next cyber-attack platform
Silowash et al., 2012	Best practices guide	Several industry, federal, and international standards	Insider threat	Describes 19 practices to prevent and detect insider threats
Sood et al., 2015	Literature review and synthesis		Attacks through socioware and insider threat	Taxonomy of malware infestations and the use of socioware by insider threats
Symantec, 2016	Best practices guide	23,980 vendors representing over 71,470 products	Cybersecurity threats	Presents best practices guidelines against Internet threats

Table 5

Literature Summary of Social Engineering (Phishing, Vishing, & Impersonation) (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Verizon, 2016	Case study	100,000 incidents, of which 3,141, were confirmed data breaches	68 contributing organizations	9 attack vectors remain prevalent in cyber-attacks, adversary actions not exclusive to any single pattern

Yeboah- Boateng & Amanor, 2014	Empirical study	Investigation of various types of attacks on mobile devices	SMishing and vishing attacks	Taxonomy of alluring and decoying words used in phishing attacks
---	--------------------	--	---------------------------------	--

Insider Threat

Malicious Insiders

According to Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005), an insider threat is one that “originating from people who have been given access rights to an information system (IS) and misuse their privileges, thus violating the IS security policy of the organization” (p. 473). Carnegie Mellon University's Software Engineering Institute (SEI) identified the malicious insider “as a current or former employee, contractor, or business partner that has or had authorized access to an organizations network, system or data” (Silowash et al., 2012). Silowash et al. (2012) further explained that malicious insiders have “intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability (CIA) of the organizations information or information systems” (p. 8). At the time of this study, insider threats have been minimally addressed by standard security practices, yet the insider poses one of the most serious threats to organizations through any number of malicious activities (Punithavathani et al., 2015). Nurse et al. (2014) noted, “it is widely accepted that there are a myriad of insider incidents that will go unreported (for fear of organizational reputation), or will go unnoticed as the attacks avoid detection” (p. 214). Due to the nature of insider threats, malicious insiders are expected to hide their actions

with techniques they believe will avoid detection, until they have accomplished their goals (Young et al., 2014).

What contributes most to malicious insiders' exigency is that they have in-depth knowledge of the inner workings of their organization, and have the necessary privileges to access sensitive information (Agrafiotis, Legg, Goldsmith, & Creese, 2014). This understanding of the insider threat vector is further supported in the literature by Ho et al. (2015) who acknowledged, "a malicious insider has the distinct advantage of understanding the corporation's information assets, processes, and infrastructure" (p. 102). Claycomb, Legg, and Gollmann (2013) noted, "consequences of insider attacks include compromised organizational security, financial loss, and risk to human health and safety" (p. 1). Malicious insiders are capable of stealing intellectual property, disrupting organizational IT systems operations, or using organizational IT systems for financial fraud operations (Claycomb et al., 2013).

Table 6

Literature Summary of Malicious Insiders

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Agrafiotis et al., 2014	Empirical study	CMU simulated data set	Cybersecurity insider threat	Proposed a sequential analysis approach for insider threat detection
Claycomb et al., 2013	Literature review and synthesis		Cybersecurity insider threat	Identified gaps in research regarding the relationship between anomalous and malicious behavior
Ho et al.,	Empirical	Online	Language	Identified the use of

2015	study	gaming environment	used in group dynamics	language cues in group dynamics after insider threat compromise
Nurse et al., 2014	Case study and literature review	Grounded theory approach based on the review of 80 insider threat cases	Cybersecurity insider threat detection	Developed a framework that identifies elements within the insider threat problem to include motivation behind malicious threats
Punithavathani, 2015	Empirical study	Real time values comprised of simulated systems	Cybersecurity insider threat detection	Developed a two-phased surveillance mechanism for insider threat detection
Randazzo et al., 2005	Aggregated case-study analysis	23 incidents carried out by 26 insiders in the financial sector	Cybersecurity insider threat detection	Information development of commonalities within the cases studied

Table 6

Literature Summary of Malicious Insiders (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Silowash, et al., 2012	Empirical study	700 insider threat cases	Cybersecurity insider threat prevention	Introduced 6 key groups necessary for a successful insider threat program
Theoharidou et al., 2005	Literature review and analysis	Criminology theories and their relation to ISO 17799	Cyber threats	Identified incorporating criminology theories into

				cybersecurity management
Young et al., 2014	Empirical study	Test database of 5,500 users	Cybersecurity insider threat detection	Developed an ensemble-based, unsupervised technique for detecting potential insider threat instances

Observable Behavior

It has also been noted in the literature that an insider attack is often preceded by observable behaviors consisting of indicators to current or future malicious behavior (Claycomb et al., 2013; Greitzer et al., 2012). In the work of Greitzer and Frincke (2010), incoming data is processed to infer observations; observations are processed to infer indicators; and indicators are assessed to gauge threat (p. 8). An example of a technical observation is data that represents the activities of an employee's network account, such as outgoing or incoming Web traffic, or data connections through a firewall per IP mapped back to the user's network account (Greitzer & Frincke, 2010). On the other hand, while more fragmented, human resources data provides a multitude of contextual, behavioral, and psychosocial information regarding employees (Costa et al., 2014). This data as outlined by Costa et al. (2014) included organizational charts, employee performance reviews, employee personnel files, employee behavior records, information from anonymous insider reporting channels, and results from background checks. The combination of several of these factors, "if properly evaluated in a timely manner, could alert an organization about a developing insider crime" (Greitzer et al., 2014, p. 109). In the work of Greitzer et al. (2012), a psychosocial model was developed to assess an

employee's increased susceptibility to becoming an inside abuser. According to Greitzer et al. (2012), in many insider threat cases, managers and coworkers observed that the offender had exhibited signs of stress, disgruntlement, or other issues, yet no one questioned the behavior or raised an alarm. This research aimed at filling that gap by introducing a mechanism within the AI-InCyThR system proof-of-concept prototype, where a combination of an employee's FFM and technical activity were input as indicators to the system. The data captured was analyzed within the proof-of-concept prototype for correlation to validate the expert panel identified indicators.

Table 7

Literature Summary of Observable Behavior

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Costa et al., 2014	Empirical study	800 insider threat cases	Cyber threat indicators	Developed an ontology for insider threat indicators
Greitzer et al., 2010	Empirical study	HR experts and managers	Cyber threat indicators	Developed a predictive modeling approach using threat indicators preceding an insider threat attack
Greitzer et al., 2014	Empirical study	Expert judgements	Psychosocial indicators	Developed a prototype psychosocial model that assess behavioral indicators

Insiders as Adversaries and Cyber Adversarial Thinking

Randazzo et al., (2005) concluded that most insiders were motivated by financial gain, and not a desire to cause harm to the organization. According to Randazzo et al. (2005), 27% of the insiders studied were experiencing financial difficulties. They also noted that “other motives included revenge, dissatisfaction with company management, culture, or policies, and a desire for respect” (Randazzo et al., 2005, p. 14). Former employees are familiar with organizational culture, policies, and procedures, which can be exploited in an insider attack (Andersen et al., 2004). For this research study, adversarial thinking was one of the indicator categorizations. Band et al. (2006) argued that the “needs” of an individual often manifest as personal disposition in the workplace and have been related to maladaptive reactions to stress, financial problems, and personal needs, leading to personal conflicts, concealment of rule violations, chronic disgruntlement, strong reaction to organizational sanctions, and a propensity for escalation in work-related issues (p. 15). While Band et al. (2006), observed personal predispositions were grouped into five categories: serious mental health disorders, personality problems, social skills and decision-making biases, as well as, a history of conflicts, these constructs are outside the scope of this study and will be incorporated into future research. Furthermore, personal predispositions appeared to play a role in both sabotage and espionage risks (Band et al., 2006).

Table 8

Literature Summary of Insiders as Adversaries and Cyber Adversarial Thinking

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Anderson et	Case study	six insider	Cybersecurity	Approach to

al., 2004		threat cases	insider threat detection	cybersecurity for organizations policies and practices
Band et al., 2006	Empirical study	49 insider threat sabotage cases	Cybersecurity insider threat sabotage detection	Developed three models that describe the relationships between insider threat sabotage and espionage
Randazzo et al., 2005	Aggregated case-study analysis	23 incidents carried out by 26 insiders in the financial sector	Cybersecurity insider threat detection	Information development of commonalities within the cases studied

Insider Threat Cases Overview

According to Moore, Collins, Mundie, Ruefle, and McIntire (2014), analysis of insider threat cases regarding IT sabotage involved remote access outside of the insiders' normal working hours. Moreover, analysis of insider threat cases show that 57% of insider threat sabotage cases involved an attack within 60 days of the insider's termination from employment with the organization (Moore et al., 2014).

At the time of this study, one of the most recent high-profile insider threat cases was that of Edward Snowden. Snowden, a former Central Intelligence Agency (CIA) employee, and later a Booz Allen Hamilton federal government consultant, had held a position that required a top secret security clearance (Kont, Pihelgas, Wojtkowiak, Trinberg, & Osula, 2015). In June, 2013, Snowden spent several months working as a high-level systems administrator before contacting Glenn Greenwald, a lawyer and journalist, to disclose an unknown number of digital documents (Kont et al., 2015). Snowden's motivation for disclosure and security breach was his concern over how much

personal data the National Security Agency (NSA) was collecting about ordinary Americans, and he believed much more was being collected than was actually necessary (Landau, 2013). The implications of Snowden’s disclosures of sensitive and classified information were of great concern to not only the U.S. government, but also its allies (Young, 2014).

Intelligence Community Standard (ICS) Number 500-27, *Collecting and Sharing of Audit Data*, provides a comprehensive list of auditable events that “support lawful and appropriate information assurance, business analytics, personnel security, and other security community audit needs” (Committee on National Security Systems, 2013).

ICS Number 700-2, *The Use of Audit Data for Insider Threat Detection*, contains information about the types of enterprise audit data that should be used as potential indicators for individuals holding a Department of Defense (DoD) security clearance (Guido & Brooks, 2013). This data can be analyzed in conjunction with other available data in support of the detection, mitigation, or assessment of insider threats. Expanding the amount and type of simulated data analyzed allowed for better insight into the individuals and situations that may lead to insider threat activity.

Table 9

Literature Summary of Insider Threat Cases Overview

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Committee on National Security Systems, 2013	Operational guidance	NIST SPs executive orders, and intelligence community standards	Information systems auditing	Annex of user / pc auditable events

Table 9

Literature Summary of Insider Threat Cases Overview (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Guido & Brooks, 2013	Literature review and synthesis	Various organizations with successful insider threat programs	Cybersecurity insider threat	Development of a straw man insider threat program model
Kont et al., 2015	Case study and literature review & synthesis	Reviews of existing insider research, and case studies	Insider threat detection and mitigation	Technical and nontechnical indicators used in the detection of insider threats
Landau, 2013	Case study and literature review	Recent insider threat attack	Cybersecurity insider threat	Complications within U.S. federal agencies and information disclosure
Moore et al., 2014	Empirical study	800 cases of malicious insider crime, 120 cases of espionage	Enterprise architecture patterns	Presentation of insider threat mitigation language
Young, 2014	Case study	Insider threat attack	Cybersecurity insider threat	Aftermath of insider attack

Cybersecurity Indicators and Categories

The Committee on National Security System Instruction (CNSSI) has outlined the minimum requirements for deploying the Enterprise Audit Management (EAM) as required by ICS-500-27, these are as shown in Table 10 (Committee on National Security Systems Instruction, 2013, p. B-1):

Table 10

Auditable Attributable Events or Activities

Auditable Events (ICS-500-27)	
Authentication Events	Logons (Success/Failure)
	Logoffs (Success/Failure)
File and Object Events	Create (Success/Failure)
	Access (Success/Failure)
	Delete (Success/Failure)
	Modify (Success/Failure)
	Permission Modification (Success/Failure)
	Ownership Modification (Success/Failure)
Writes/downloads to external device/media (e.g., A-Drive, CD/DVD, devices/printers)	(Success/Failure)
Uploads from external devices (e.g., (CD/DVD drives)	(Success/Failure)
User and Group Management events	User add, delete, modify, suspend, lock (Success/Failure)
	Group/Role add, delete, modify (Success/Failure)
Use of Privileged/Special Rights events	Security or audit policy changes (Success/Failure)
	Configuration changes (Success/Failure)
Admin or root-level access	(Success/Failure)
Privilege/Role escalation	(Success/Failure)
Audit and log data accesses	(Success/Failure)
System reboot, restart and shutdown	(Success/Failure)
Print to a device	(Success/Failure)

Table 10

Auditable Attributable Events or Activities (Cont.)

Print to a file (e.g., pdf format)	(Success/Failure)
Auditable Events (ICS-500-27)	
Application (e.g., Firefox, IE, MS Office, etc.) initialization	(Success/Failure)
Export of information (e.g., to CDRW, thumb drives, or remote systems)	(Success/Failure)
Import or information including (e.g., to CDRW, thumb drives, or remote systems)	(Success/Failure)
Auditable Event Details Information Events (Splunk, 2014, p. 5)	
Date and time of the event using common network time (Network Time Protocol (NTP) Protocol)	
Type of event (e.g., login, print, etc.)	
Identifier indicating the source system of the event activity	
Identifier indicating the identity of the subject or actor (e.g., UserID, ProcessID, etc.)	
Details identifying any object or resources accessed or involved (aka Resource list, e.g., files (including location), document ID, peripherals, storage devices etc.)	(Success/Failure)
Attributable Events Indicating Violations of System/Target (events of concern requiring further analysis or review.) (CNSS, 2013, p. B-2)	
Malicious code detection	
Unauthorized local device access	
Unauthorized executable	

Table 10

Auditable Attributable Events or Activities (Cont.)

Attributable Events Indicating Violations of System/Target (events of concern requiring further analysis or review.) (CNSS, 2013, p. B-2)
Unauthorized privileged access
System reset/reboot
Disabling the audit mechanism
Downloading to local devices

These requirements are a culmination of several federal directives, executive orders, other standards, and NIST guidelines. These lists and guidelines are important as they are recommended actions and operational guides to users, IT staff, security staff, and others, when specific standards won't apply (Harris, 2013). At the time of this study, developments in cloud technologies have allowed employees and organizations to have more flexibilities in how they work, allowing for working remotely to become more accepted. That being said, the 2015 American Time Use Survey issued by the U.S. Department of Labor, Bureau of Labor Statistics (U.S. Department of Labor, 2016), showed that telecommuting is approximately 24% of employee's telework with some frequency. That being said, about 82% of employees are working within the organizational boundary. This study focused on the activity of the majority of employees, as noted by report above, that are behind the firewall and within the organizational boundary.

Table 11

Literature Summary of Cyber Threat Indicators and Categories

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Committee on National Security Systems, 2013	Operational guidance	NIST, executive orders, and intelligence community standards	Information systems auditing	Annex of user / pc auditable events
Harris, 2013	Instructional		Industry standards	Instruction for CISSP certification
Splunk, 2014	Situational awareness		Industry standards	ICS 700-2 and indicators for insider threat
U.S. Department of Labor, 2016	Operational guidance	10,099 individuals interviewed	Industry practices	How individuals over 15 spent their time

Incident Response

Tondel, Line, and Jaatun (2014) explained that, based on International Standards Organization (ISO) and National Institute of Standards and Technology (NIST) guidelines, an information security event can be described as an occurrence within a system, service, or network state, that indicates a possible breach of security, outlined policy, or failure of implemented controls, as well as, a previously unknown situation that may be relevant to main security. As noted by Grispos, Bradley, and Storer (2015), “researchers and industrial analysts contend that there are fundamental problems with the existing security incident response process solutions” (p. 1). Ruefle et al. (2014)

demonstrated that organized incident management involves organizationally defined, repeatable processes with the ability to learn from the identified incidents that threaten organizational computer systems and data. In most organizations, computer incidents are managed by a computer security incident response team (CSIRT). Metzger, Hommel, and Reiser (2011) reasoned that the CSIRT is enabled to correlate IT-related security events across various communications channels and classify incidents in a consistent manner. Therefore, depending on the incident classification, either manual or automated reaction steps can be taken, either by an automated notification email to network and security administrators, or a full segregation of a compromised system or network (Metzger et al., 2011).

Recommendations by NIST researchers Cichonski, Millar, Grance, and Scarfone (2012) outlined in their computer security incident handling guide four key phases in the computer incident response cycle:

1. “Preparation
2. Detection and analysis
3. Containment/eradication
4. Recovery, and post-incident activity.” (p. 21)

As seen in Figure 2, the incident response phases relate to each other in a cyclical manner, supplementing continuous monitoring and improvement. Further requirements as outline by NIST include:

1. “Creating an incident response policy and plan
2. Developing procedures for performing incident handling reporting

3. Setting guidelines for communicating with outside parties regarding incidents
4. Selecting a team structure and staffing model
5. Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
6. Determining what services the incident response team should provide
7. Staffing and training the incident response team.” (Cichonski et al, 2012, p. 21)

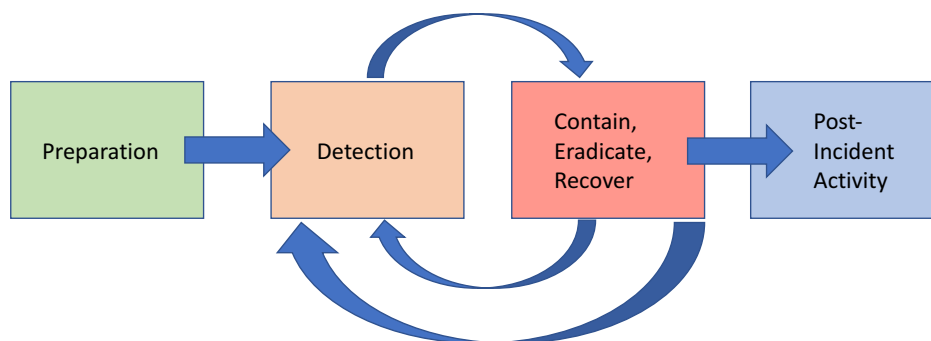


Figure 2. Incident Response Life Cycle (Cichonski et al., 2012)

According to Grispos et al. (2011), in the event of an incident, the CSIRT gathers forensic data from multiple sources, which can include logs, emails, hard drive images, and physical memory dumps. Once specific tool designed to support information security professionals, is known as intrusion detection system (IDS) (Werlinger, Muldner, Hawkey, & Beznosov, 2010). The incident diagnostic process begins with a preparation phase, which includes knowledge-gathering about vulnerabilities and risks through the use of tools such as the IDS (Werlinger et al., 2010).

Table 12

Literature Summary of Incident Response

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Cichonski et al., 2012	Guidelines		Computer security incident response	Guidelines to assist in establishing computer security incident response capabilities
Grispos, 2015	Literature review and empirical study	15 individuals surveyed in semi-structured interviews	Cybersecurity incident response	Organizations can benefit from an alternative approach to incident handling and managing security incidents
Metzger et al., 2011	Empirical study	Munich scientific network, 120,000 users, 80,000 devices	Cybersecurity incident response	Various reporting capabilities can be leveraged for effective, efficient, and integrated incident response
Ruefle et al., 2014	Theoretical		Computer security incident response team (CSIRT) development	Defined incident response management via CSIRT ensure focused incident response efforts

Table 12

Literature Summary of Incident Response (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Tondel et al., 2014	Empirical study	6 individuals surveyed in semi-structured interviews	Information security incident response	Incident planning and preparation differ for IT and industrial control systems a unified approach for critical infrastructure

Intrusion Detection and Prevention Systems (IDPS)

The IDPS is defined a software application that has the ability to monitor network and system activities for unauthorized users and activities, as well as, alert organizational personnel of such activities, including suspicious inbound and outbound traffic (Vaidya, Mirza, & Mali, 2010). According to Scarfone and Mell (2007), “intrusion prevention is the process of performing the process of intrusion detection and attempting to stop possible incidents” (p. ES-1). Patrick (2001) illustrated how IDPS helps information systems prepare for and deal with attacks, by noting that “this is accomplished by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems” (p. 3). Patrick (2001) further elaborated on the benefits that IDPS provide, including: monitoring and analysis, auditing of systems, configurations and vulnerabilities, system integrity, analysis of activity patterns based on the matching to known attacks, abnormal activity analysis, and operating system audits.

One of the main points of this study was to identify abnormal or anomalous user activity in an attempt to discover precursor activities to insider threat behavior.

According to Brown, Suckow, and Wang (2002), anomaly detection is concerned with identifying events that appear to be anomalous with respect to normal user behavior on the system. This research and proof-of-concept development aimed to identify anomalous user behavior through linear and non-linear models of username and expert panel-defined input indicators, through the analysis of input indicator associations or clustering.

Table 13

Literature Summary of Intrusion Detection and Prevention Systems

Study	Methodology	Sample	Instrument of Construct	Main Finding or Contribution
Broan et al., 2002	Literature review and analysis		Intrusion detection systems	Identified IDS characteristics and training behavioral models
Patrick, 2001	Literature review and analysis		Successful IDS implementation	Identified best practices to successfully implement an ISD within an organization
Scarfone & Mell, 2007	Recommendations and standards		Intrusion detection and prevention systems	Recommendations for designing, implementing, configuring, securing, monitoring, and maintaining IDPS

Table 13

Literature Summary of Intrusion Detection and Prevention Systems (Cont.)

Study	Methodology	Sample	Instrument of Construct	Main Finding or Contribution
Li & Datardina, 2010	Literature review		Intrusion detection systems	Provided information on intrusion detection approaches and technologies

Security Information and Event Management (SIEM) Solutions

Cyber attacks have become increasingly more sophisticated, making traditional log management and monitoring tools insufficient for the detection, prevention, and mitigation of cyber attacks. This elicits a need for more efficient and effective event intelligence, as well as, deeper analysis and understanding of environments with the use of security information and event management (SIEM) platforms (Thakur, Kopecky, Nuseir, Ali, & Qiu, 2016). One of the benefits of SIEM technology is its ability to analyze security event data in real time, and its ability to collect, store, analyze, and report on logged data for regulatory compliance along with forensics (Montesino, Fenz, & Baluja, 2012, p. 249). Montesino, Fenz, and Baluja (2012) outlined the major functions of the SIEM technologies:

Security information management (SIM): Log management and compliance reporting. The SIM service provides the collection, reporting, and analysis of various log source data, primarily from host systems and applications, and secondarily from network and security devices in support of regulatory

compliance reporting, threat management, and organizational resource monitoring (Montesino et al., 2012, p. 253).

Security event management (SEM): Real-time monitoring and incident management for security-related events. The SEM service processes logs and event data from security devices, network devices, systems, as well as, applications in real-time to security monitoring, activity correlation and incident responses (Montesino et al., 2012, p. 253).

IDPS and SIEM tools merely scratch the surface in detecting cyber threats to an organization's infrastructure, simply because the number and sophistication of attacks keep rising, making even the security tools themselves vulnerable to attacks (Thakur et al., 2016).

Table 14

Literature Summary of Security Information and Event Management (SIEM) Solutions

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Montesino et al., 2012	Empirical study	NIST 800-53 and ISO.IEC 27001 security controls	Cybersecurity automation	Finds that 30% of NIST 800-53 security controls can be automated
Thakur, 2016	Conceptual study	HP ArcSight SIEM application	Security event and log management	Best practices in enterprise security management

System Security Baseline Standards and Guidelines

Aim and Scope of a Security Policy

According to Backhouse, Hsu, and Silva (2006), when considering information systems security, “standards are fundamental compatibility specifications that shape the configuration of information systems” (p. 413). The scope of a standard depends on the immediate needs of the organization, and will specify a standard for installing, hardening, and placing systems into production (Livingston, 2000). Livingston (2000) further explained that a Minimum Security Baseline Standard (MSB) allows organizations to deploy systems in more controlled, efficient, and standardized manner (p. 1). In IT and security, the use of baselines has far-reaching effects, as they provide a measuring point from which a comparative analysis can be derived, both before and after any changes or incidents to a systems occurred (Fuller & Atlasis, 2012). NIST SP 800-53 (2013) explained that one of the most significant challenges for organizations is in determining the most cost-effective and appropriate set of security controls, which, if implemented properly, would mitigate risk while helping to comply with federal laws, standards, and other directives. To further expand on NIST SP 800-53 in order to assist organizations in making the appropriate security control selection for their IT, the concept of “baseline controls” was introduced (NIST, 2013). These controls act as a starting point for security implementation, based on system criticality and associated risk, along with impact level.

In response to Presidential Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” NIST developed the Cybersecurity Framework (2014) through a collaboration between the Federal Government and private industry, while it is intended to complement an organization’s risk management and cybersecurity program using common language in a cost-effective manner, without placing regulatory

requirements on businesses (NIST, 2014). As outlined by AT&T Security (2015), information security is not just a top executive or IT issue.

Table 15

Literature Summary of Aim and Scope of a Security Policy

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
AT&T Security, 2015	Conceptual paper		Industry best practices	Security must be viewed with many lenses
Backhouse et al., 2006	Case study	11 structured interviews with email follow up	Perceived power	Theoretical framework revealing levels of jurisdiction in which actors operate
Fuller & Atlasis, 2012	Literature review and analysis		IT professional competence	Specific IT/cybersecurity system baselining procedures
Livingston, 2000	Literature review and analysis		IT professional competence	Specific IT/cybersecurity minimum security baselining procedures

Cybersecurity Monitoring

Insider Technical Event Indicators

Creasy and Glover (2015) of the Council of Registered Ethical Security Testers (CREST), an international certification and accreditation body for the technical information security industry, identified four types of technical event logs that can be

useful for cybersecurity monitoring, and assist with the detection of potential cybersecurity incidents (p. 18). Table 16 outlines the recommended log types and examples for technical cybersecurity indicators. As noted by Verizon (2010), while it is never a good thing to have large amounts of data leave a network at any given time, this can indicate malicious activity. Looking for the correct indicators in the correct locations can help mitigate a situation before it escalates into an event or a cyber-attack. By applying different analytical techniques, cybersecurity analysts can validate the quality of the information collected to identify indicators of actualized threats (Young, 2014).

Table 16

Technical Cybersecurity Indicators

Types of Logs	Examples
System logs	System activity logs (Administrator), including storage Endpoint and agent based logs Logs from standard and customized applications Authentication logs Physical security logs
Network logs	Email, firewall, VPN, and Netflow logs
Technical logs	HTTP proxy logs DNS, DHCP, and FTP logs Web and SQL logs Appflow logs

Table 16

Technical Cybersecurity Indicators (Cont.)

Types of Logs	Examples
Logs from cybersecurity monitoring and logging tools	Malware protection (anti-virus) logs
	Intrusion detection and prevention systems (IDPS) logs
	Data loss protection (DLP) logs
	Tools that employ potential malware isolation and investigation (sandbox or virtual execution engines)
	Other relevant security management appliances or tools.

According to Creasy and Glover (2015), event logs and tools should be configured to enable event logging, use standard formats such as syslog, be parsed with the necessary attributes (IP, user name, time & date, protocol, & port), and use a consistent, trusted date and time source, such as Network Time Protocol (NTP) (p. 18).

Table 17

A Summary of Insider Technical Event Indicators

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Creasy & Glover, 2015	Industry best practices to help capture important cybersecurity events	Consumer organizations, government bodies, and academia	Cybersecurity threat identification	Details on how to monitor and log cybersecurity events
Verizon, 2010	Cybersecurity breach investigation and analysis	141 confirmed breaches	Cybersecurity threat identification	Identification of preventive measures divided into categories

Table 17

A Summary of Insider Technical Event Indicators (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Young, 2014	Case study	Insider threat attack	Cybersecurity threat identification	Techniques to validate threat information

Insider Personality and Human-Centric Indicators

Greitzer et al. (2010) discussed several demographic, behavioral, or psychosocial data, which, if used in various combinations, could provide warning signs of malicious insider threats (p. 13). According to Barrick and Mount (1993), “it has long been argued that the relationship between personality characteristics and behavior is moderated by the strength (or demands) of the situation” (p. 112). They further explained this to mean that the extent to which individuals’ personality characteristics predict behavior differs “depending on the degree to which the external environment inhibits a person’s freedom to behave in idiosyncratic ways” (p. 112). As noted by DeYoung (2015), researchers in the psychology field often refer to “personality” as the “array of constructs that identify variables in which individuals differ” (p. 33). In addition, personality refers to the “specific mental organization and processes that produce an individual’s characteristic patterns of behavior and experience” (DeYoung, 2015, p. 33). McAdams and Pals (2006) explained that the mission of personality research is “to provide an integrative framework for understanding the whole person” (p. 204). DeYoung (2015) described personality

traits as “probabilistic descriptions of relatively stable patterns of emotion, motivation, cognition, and behavior in response to classes of stimuli” (p. 35). In insider threat research it is important to understand to the whole person because as noted by Greitzer et al. (2014), “findings from research and case studies of insider crime suggests the presence of personality predispositions in perpetrators” (p. 121).

The Five Factor Model of Personality

McCrae and Costa (2008) explained that the FFM of personality is the empirical generalization about the covariance of personality traits (p. 159). Also referred to as the Big Five, FFM “organizes broad individual differences in social and emotional life into five factor-analytically-derived categories” (McAdams & Pals, 2006, p. 204). According to Pytlik Zillig, Hemenover, and Dienstbier (2002), the FFM of personality: Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism (OCEAN), have emerged from decades of research and are notable for their ability to simplify the vast number of traits, and ability to predict certain outcomes (p. 847). According to McCrae and Costa (1991), the FFM is comprehensive and provides a basis for a systemic study of personality and affect (p. 227). Therefore, the FFM constructs and general descriptions listed in Table 18, were used in this research study as indicators to determine the strength of relationships between personality factors and malicious technical activity.

Table 18

Human-centric Indicators - Five Factor Model of Personality

Indicator	Description	Author(s)
Openness	Imaginative, artistically sensitive, intellectual; creative, thoughtful	Barrick & Mount, 2010; Judge & Bono, 2000

Table 18

Human-centric Indicators - Five Factor Model of Personality (Cont.)

Indicator	Description	Author(s)
Conscientiousness	Responsible, dependable, persistent, achievement oriented	Barrick & Mount, 2010; Judge & Bono, 2000
Extraversion	Outgoing, active, sociable, talkative, assertiveness	Barrick & Mount, 2010; Judge & Bono, 2000
Agreeableness	Good-natured, cooperative, kind, gentle, trusting	Barrick & Mount, 2010; Judge & Bono, 2000
Neuroticism	Tense, insecure, nervous; anxious, fearful, depressed, moody	Barrick & Mount, 2010; Judge & Bono, 2000

As noted earlier, the FFM is a hierarchical model of personality traits encompassing five factors representing personality at the broadest level, and is considered the dominant approach for representing the human trait structure (Gosling, Rentfrow, & Swann, 2003; Roccas, Sagiv, Schwartz, & Knafo, 2002). As explained by McAdams and Pals (2006), when “taken together, the five principles assert that dispositional traits articulate broad variations in human functioning that are recognizable, speaking directly to how human beings respond to situated social tasks” (p. 205).

In addition to the Human-centric psychometric indicators outlined, time working at an organization has also been studied within the private and public sectors (Ramim & Levy, 2006; Hoffman, Meyer, Schwarz, & Duncan, 1990). As noted by Mullen (1981), the largest percentage of insider threat incidents, 38%, occurred during the six to 10-year period of employment, this is followed by 27% in the three to five-year time period, with

19% of insider threat incidents occurring within the first two years of employment.

Hoffman, Meyer, Schwarz, and Duncan (1990) determined that long term employment at an organization does not guarantee that employees will not be tempted to malicious activity. In their study, Hoffman et al., (1990) discovered that four out of the 62 insider threat cases reviewed, had been at their place of employment for over 10 years.

Table 19

Literature Summary of Insider Personality and Human-Centric Indicators

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Barrick & Mount, 1993	Empirical study	154 participants	Personality scales from several personality inventories	Mean, standard deviations, reliabilities, correlations for job level measures
DeYoung, 2015	Literature review and synthesis		Cybernetics and FFM in goal directed systems	Introduction of Cybernetic Big-Five theory
Gosling et al., 2003	Empirical study	1704 undergrad student participants	External correlates of a new Ten Item Personality Inventory (TIPI)	Introduction of TIPI as a short measure for FFM psychometrics
Greitzer & Ferryman, 2013	Empirical study	Word analysis representing 167 senders, and 5.25 million words	Insider threat mitigation	Analytic approaches and metrics in evaluating tools to identify insider threats

Table 19

Literature Summary of Insider Personality and Human-Centric Indicators (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Greitzer et al., 2010	Empirical study	10 staff members recommended by HR, reviewed 24 insider threat cases	Insider threat prediction	Validation using twelve indicators and a good model, insider threat risk can be correlated with HR judgements
Hoffman et al., 1990	Empirical study	62 insider threat cases	Insider threat prediction	Impact of insiders working with outsiders to bring harm to nuclear facilities.
Judge & Bone, 2000	Empirical study	316 participants enrolled in a community program	Linking FFM to transformational leadership	Agreeableness as strong predictor of leadership behavior
McAdams & Pals, 2006	Literature review and synthesis		FFM, individual traits and characteristics	Principles for integrating the science of personality
McCrae & Costa, 1991	Empirical study	429 participants in a longitudinal study	FFM and wellbeing	Effects of personality on psychological wellbeing
McCrae & Costa, 2008	Theoretical		FFM and Trait Theory	Dimensions of FFM personality traits and human nature

Table 19

Literature Summary of Insider Personality and Human-Centric Indicators (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Lytlik Zillig et al., 2002	Literature review and synthesis		Personality inventory samples	New perspectives on FFM and the nature of personality traits
Ramim & Levy, 2006	Case study	Small university setting	Insider cyber attack	Insider cyber attack was successful do to novice IT management and lack of policies and governance
Mullen, 1981	Empirical study	650 articles, studies, and books	Insider threat characteristics	Provided a set of insider threat characteristics and potential threats to nuclear facilities
Roccas et al., 2002	Empirical study	246 introductory psychology students	FFM and personal values	Relating FFM and basic personal values

Delphi Technique

According to Straub (1989), content validity is established by literature reviews, a pretest phase, and use of expert panels. Lichvar (2011), noted that an expert is a specialist in his or her particular field or domain. Furthermore, as explained by Sekaran and Bougie (2013), an expert panel can verify that the measures being employed truly include “an adequate and representative set of items that tap the concept” (Sekaran & Bougie, 2013, p. 226). Okoli and Pawlowski (2004) indicated that when judgmental information is

essential, researchers should employ the Delphi technique. The Delphi technique “involves the repeated individual questioning of the experts (by interview or questionnaire) and avoids direct confrontation of the experts with one another” (Dalkey & Helmer, 1963, p. 458). Linstone and Turnoff (2002) characterized the Delphi technique as “a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem” (p. 3). Prior research, e.g. Ramim and Lichvar (2014), Tracey and Richey (2007), as well as Schmidt, Lyytinen, Keil, and Cule (2001) applied the Delphi technique for issue identification, model forecasting, and the development of the conceptual framework. According to Schmidt et al. (2001), the Delphi technique ensures “a reliable and validated data collection process” (p. 10) by compiling often contradictory opinions, while pursuing a consolidation of the experts’ responses. This research study identified the expert opinions of malicious cybersecurity insider threat indicators through the use of the Delphi technique.

Table 20

Literature Summary of Delphi Technique

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Dalkey & Helmer, 1963	Theoretical		Delphi techniques and application	Determined Delphi is conducive in producing insights into the subject matter

Table 20

Literature Summary of Delphi Technique (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Lichvar, 2011	Empirical study	256 respondents	7-part survey instrument	Validate the effects of knowledge sharing
Linstone & Turnoff, (2002)	Theoretical		Delphi techniques and application	Delphi method for group communication process
Okoli & Pawlowski, (2004)	Theoretical		Delphi techniques and application	Uses of the Delphi technique for theory building
Ramim & Lichavar, 2014	Theoretical		Delphi techniques and application	Uses of Delphi technique in project management
Schmidt et al., (2001)	Empirical study	6616 respondents	Delphi survey	Improving risk management practices
Straub, (1989)	Theoretical		Instrument validation	Overview of the basic principles of instrument validation
Tracey & Richey, (2007)	Empirical study		Model construction and validation	Decision-making processes and procedures in model development

Data Mining

Data mining enables researchers to find information that was not expected to be revealed in databases (Clifton & Marks, 1996). According to Hearst (1999), “the goal of data mining is to discover or derive new information from data, finding patterns across datasets, and/or separating signal from noise” (p. 3). Additionally, data mining is often referred to as “knowledge discovery” in databases, meaning “the process of nontrivial extraction of implicit, unknown, and potentially useful information from data” (Chen, Han, & Yu, 1996, p. 1041). Chen et al. (1996) elaborated on data mining, in that discovered knowledge can be applied to inform management and assist in the decision making process, as well as, many other applications. An objective of data mining, or data exploration, is to find correlations in the data and uncover hidden patterns within the data distribution to provide more insight into the data (Reddy & Aziz, 2010).

Table 21

Literature Summary of Data Mining

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Chen et al., 1996	Literature review and analysis		Cybersecurity and Privacy issues in critical infrastructure	Methodology for data analysis and research on vulnerabilities in smart grid and critical infrastructure
Clifton & Marks, 1996	Theoretical		Data mining techniques to summarize data	The use of public and sensitive information in search of inference paths

Table 21

Literature Summary of Data Mining (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Hearst, 1999	Theoretical		Data mining for text exploration	Text exploration strategies
Reddy & Aziz, 2009	Theoretical	Several real-world datasets	Nonlinear data correlations	Method for computing subspace principal curve models

Pattern Recognition

As explained by Raj, Swaminarayan, Saini, and Parmar (2015), “a pattern can have a perceptual feature, a way of operation or behavior, something regarded as a normative example, or a model considered worthy of imitation” (p. 2496). According to Bishop (2006), pattern recognition pertains to “the automatic discovery of regularities in data through the use of computer algorithms, and with the use of these regularities to take action, such as classifying the data into different categories” (p. 1). The concept behind pattern recognition is to assign labels to objects, allowing a set of measurements, also called *attributes* or *features*, to describe the object (Kuncheva, 2004). Jain, Duin, and Mao (2000) explained that pattern recognition pertains to both supervised and unsupervised classification.

When considering the “unsupervised” category, which is also called *unsupervised learning*, the interest is in discovering any structure in the data, such as groups, or any shared characteristics, making the objects similar or different across the groups

(Kuncheva, 2004). According to Sathya and Abraham (2013), “unsupervised” refers to the ability to learn and organize information without providing an error signal to evaluate the potential solution” (p. 3). One advantage of unsupervised learning is that the lack of direction in the learning algorithm allows researchers to look backwards for patterns that may have not previously been considered (Kohonen, Oja, Simula, Visa, & Kangas, 1996).

Another consideration in pattern recognition is the “supervised” category, also called *supervised learning*. In supervised learning, each object in the data set has a preassigned class label. The task here is to “train a classifier to do the labeling sensibly; we supply the machine with learning skills and present the labeled data to it” (Kuncheva, 2004, p. 3). Supervised learning is efficient in that it is based on training a data sample from a data source with the correct classification already assigned; helping to find solutions to “several linear and non-linear problems such as classification, control, forecasting, and prediction” (Sathya & Abraham, 2013, p. 34).

Table 22

Literature Summary of Pattern Recognition

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Bishop, 2006	Theoretical		Pattern recognition	Overview of linear models

Table 22

Literature Summary of Pattern Recognition (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Jain, 2000	Theoretical		Statistical pattern recognition	Overview of supervised and unsupervised classification
Kohonen et al., 1996	Literature review		Data visualization	Introduced self-organizing map as a tool for data visualization
Kuncheva, 2004	Theoretical		Pattern recognition	Overview of the pattern recognition cycle
Raj, 2015	Literature review		Pattern recognition algorithms	Pattern recognition algorithms can be applied in the agricultural domain
Sathaya, 2013	Empirical study	Dataset with 300 students	Unsupervised and supervised machine learning models	Presented a conceptual framework of pattern classification in the education industry

Trend Analysis

According to Alexandrov, Bianconcini, Dagum, Maass, and McElroy (2012), there is often a need to determine if a trend exists within a given time series. This is referred to as *trend detection* and is typically solved through the use of statistical tests,

which often require the use of trend models (Alexandrov et al., 2012). As explained by Kivikunnas (1993), trends have meaning to human experts, and are patterned or structured in one-dimensional data (p. 1).

Trend analysis builds an integrated model using the following four major components or movements to characterize time-series data:

1. Trend or long-term movements: These indicate the general direction in which a time-series graph is moving over time.
2. Cyclical movements: These are long-term oscillations about a trend line or curve.
3. Seasonal variations: These are nearly identical patterns that a time series appears to follow during corresponding seasons of successive years.
4. Random movements: These characterize sporadic changes due to chance events (Han, Kamber, & Pei, 2012).

Trend analysis assists in providing context and value to either stored or real-time data. As noted by Streibel (2008), the more meaningful the stored information, the more powerful the knowledge retrieved becomes. This research study utilized pattern recognition and trend analysis techniques to identify correlations between user activity and precursors to malicious cybersecurity insider threat attacks.

Table 23

Literature Summary of Trend Analysis

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Alexandrov et al., 2012	Literature review		Trend extraction	Approaches to trend extraction for time series

Table 23

Literature Summary of Trend Analysis

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Han et al., 2012	Conceptual instruction		Data mining	Presented data mining techniques and algorithms
Kivikunnas, 1993	Literature review		Trend analysis	Identified trend analysis methods and applications
Streibel, 2008	Conceptual instruction		Data mining text	Presented data mining by analyzing text streams

Data Modeling and Simulation

By definition, “a data model is a conceptual representation of the data structures that are required by a data” (Mamcenko, 2004, p. 5). According to Navathe (1992), “a data model is a set of concepts that can be used to describe the structure of and operations on a database, meaning, data types, relationships, and other constraints within the database” (p. 113). In their seminal work, Greitzer and Frinke (2010) proposed that research should focus on: combining traditionally monitored information security data (e.g. workstation & Internet activity) with other kinds of organizational and social data to infer the motivations of individuals and predict the actions that they are undertaking, which may allow early identification of high-risk individuals (p. 2).

According to Riley (2010), one of the ways that data modeling can assist in the development of cybersecurity tools, such as the AI-InCyThR proof-of-concept prototype, uses existing computational capability to test continually security assumptions on existing

systems (p. 6). Furthermore, when dealing with cybersecurity tool development, the use of simulations or virtual machines provides a well-defined testing environment to explore, in a controlled manner, the behavior of computational and security systems in the presence of well-defined attacks (Riley, 2010, p. 6). In the work of Yan, Chen, Eidenbenz, and Li (2007), a simulation was used to study trace-oriented malware propagation using real world data.

Table 24

Literature Summary of Data Modeling and Simulation

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Mamcenko, 2004	Presentation of database management technology		IT professional competence	Specific IT database management skills
Myers et al., 2009	Literature review and synthesis		Intrusion detection system and algorithm, heuristics, and signatures	Best practices correlated with IDS algorithms for detecting malicious activity
Navathe, 1992	Literature review and synthesis		IT professional competence and database management systems (DBMS)	Proposed the classification of data models and identified specific features
Riley, 2010	Case study and game theory	Guidance from other sciences	IT and cybersecurity professional competence	Several sub-fields of computer science that are relevant in cybersecurity

Table 24

Literature Summary of Data Modeling and Simulation (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Yan et al., 2007	Empirical research	Dataset of 65,770 social media users	Trace driven simulation to study malware propagation	Trace driven simulation to study the impact of initial infection, user click probability, and user activity patterns on malware in social networks

Cross-Validation, the Bootstrap, and the Jackknife

According to Efron and Gong (1983), “cross-validation is a way of obtaining nearly unbiased estimators of prediction error in complicated situations” (p. 37). As explained by Efron and Gong (1983), the method consists of a four-step computational process which consists of:

- “(a) deleting the points x_i from the data set one at a time;
- (b) recalculating the prediction rule on the basis of the remaining $n - 1$ points;
- (c) seeing how well the recalculated rule predicts the deleted point; and
- (d) averaging these predictions over all n deletions of an x_i .” (p. 37)

The major advantage of cross-validation is that is can be applied arbitrarily to complicated prediction rules (Efron & Gong, 1983).

As noted by Efron, Halloran, and Holmes (1996), the bootstrap “is a computer-based technique for assessing the accuracy of almost any statistical estimate” (p. 13429-

13434). Orloff and Bloom (2014) further explained that the bootstrap would not be possible without current-day computing power, where the “key is to perform computation on the data itself to estimate the variation of statistics that are themselves computed from the same data” (p. 1). Additionally, according to Kleijnen and Deflandre (2005), “bootstrapping implies resampling with replacements of a given sample” (p. 123). Furthermore, bootstrapping is considered a fast analytical technique which requires an extremely short period of time to derive statistical conclusions (Kleijnen & Deflandre, 2005).

Equally important, the jackknife is a “technique for reducing the bias of a serial correlation estimator based on splitting the sample into two half-samples” (Miller, 1974) (p. 1). According to Efron (1979), “the jackknife is a nonparametric method for estimating the bias and variance of a statistic of interest, and also for testing the null hypothesis that the distribution of a statistic is centered on some pre-specified point” (p. 1). Efron and Gong (1983) illustrated that, similarly to the bootstrap, “the jackknife can be applied to any statistic that is a function of n independent and identically distributed variables” (p. 39). According to Stone (1974), jackknifing is differentiated cross-validation in that jackknifing “manufactures pseudovalues for the reduction of bias” (p. 112). However, it has been noted by Gong (1986) that, in comparing the performance of all three methods, cross-validation and jackknifing do not seem to offer any significant improvements over the apparent error rate, “whereas the improvement given by the bootstrap is substantial” (p. 108).

Table 25

Literature Summary of Cross-Validation, the Bootstrap, and the Jackknife

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Efron, 1979	Theoretical		Jackknife as a linear expansion method	Jackknife and bootstrap methods for estimating the variance the sample
Efron & Gong, 1983	Theoretical		Parametric analysis	Expository review of nonparametric estimation of statistical error
Efron et al., 1996	Theoretical		Statistical inference	As few as 50 or 100 bootstrap replications can give useful estimates.
Gong, 1986	Empirical study	Simulations and real data	Cross-validation and prediction rules	Comparison of cross-validation, jackknife, and bootstrap, show substantial gains and improvement in prediction.
Kleijnen & Deflandre, 2005	Experimental design		Monte Carlo simulations	Identified that bootstrapping validation statistics yielded distribution free confident intervals
Miller, 1974	Theoretical		Multi-sample jackknives	Two jackknife methods tested prove to be equally valid asymptotically

Table 25

Literature Summary of Cross-Validation, the Bootstrap, and the Jackknife (Cont.)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Orloff & Bloom, 2014	Conceptual paper		Empirical bootstrap methods	Outlined a set of competencies useful in statistical testing methods
Stone, 1974	Theoretical		General framework	Illustrated the application of a cross-validation criterion to the choice and assessment of statistical predictions

A Summary of What was Known and Unknown in Research Literature

A review of the literature was performed to provide an overview of the various aspects of cybersecurity, technical and human centric indicators, data simulations, and insider threats. Through this literature review, various indicators and identification models for the insider threat problem were determined, leading to the discovery of what was known and unknown in insider threat precursor identification at the time of this study. The literature has shown that, in many insider threat attacks, managers and other co-workers had observed that the individual committing the insider threat attack had exhibited signs of stress as well as disgruntlement, or other observable, unfavorable behavior, yet no one raised an alarm (Greitzer et al., 2012). These psychosocial or behavioral indicators that might be observed before an insider commits an attack can be leveraged to assist in the identification of precursors to malicious cybersecurity insider threat attack.

In the work of Greitzer et al. (2010), a model focusing on behavioral observables that could be recorded and audited was developed, helping in “making inferences about the possible psychological/personality/social state of employee” (p. 4.9). For the purposes of this study, these psychosocial indicators were not only be correlated with technical indicators and simulated user activity, but also weighted and validated by industry experts. A tool that can aggregate, in real-time, these psychosocial indicators, and correlate them with technical indicators, as well as user network activity, appeared to be absent from the literature. Thus, this study designed, developed, and empirically tested a tool that will correlate weighted and validated psychosocial behaviors/indicators with technical indicators that include network activity.

Chapter 3

Methodology

Overview of Research Design

This study was a developmental research study. As outlined by Ellis and Levy (2009) developmental research aims at answering how the construction of a “thing,” or an artifact, will address a given problem. Klein (2014) explained that design and development research is “a type of inquiry unique to the instructional design and technology field dedicated to the creation of new knowledge and the validation of existing practice” (p. 1). Ellis and Levy (2009) summarized developmental research as comprising three major elements: 1) that the product criteria must be established and validated, 2) that the product development follows formalized and accepted processes, and 3) validation of the product criteria is met through formalized, accepted processes.

Tracey and Richey (2007) used a systematic process to develop an instructional design model that was validated using the Delphi technique, where a panel of experts both analyzed and offered feedback on the researchers’ proposed design. Once the initial model was constructed, it was then reviewed and validated by industry experts through a multi-round Delphi technique (Tracey, 2009).

To meet the specific goals that address the main research question, this study conducted three phases of research as shown in Figure 3. In Phase 1, Delphi 1 and Delphi 2 were performed using instances of the Delphi technique, where SMEs validate indicators and indicator categories as well as assign indicator weights and correlations. Phase 2 of this research study consisted of in depth data analysis of the simulated employee activity data set to determine false positives and negatives, as well as, identify

significant indicators to identify insider threat activity. Phase 3 of this research study analyzed the evidence collected, and detected the accuracy of the proof-of-concept prototype predicted malicious events.

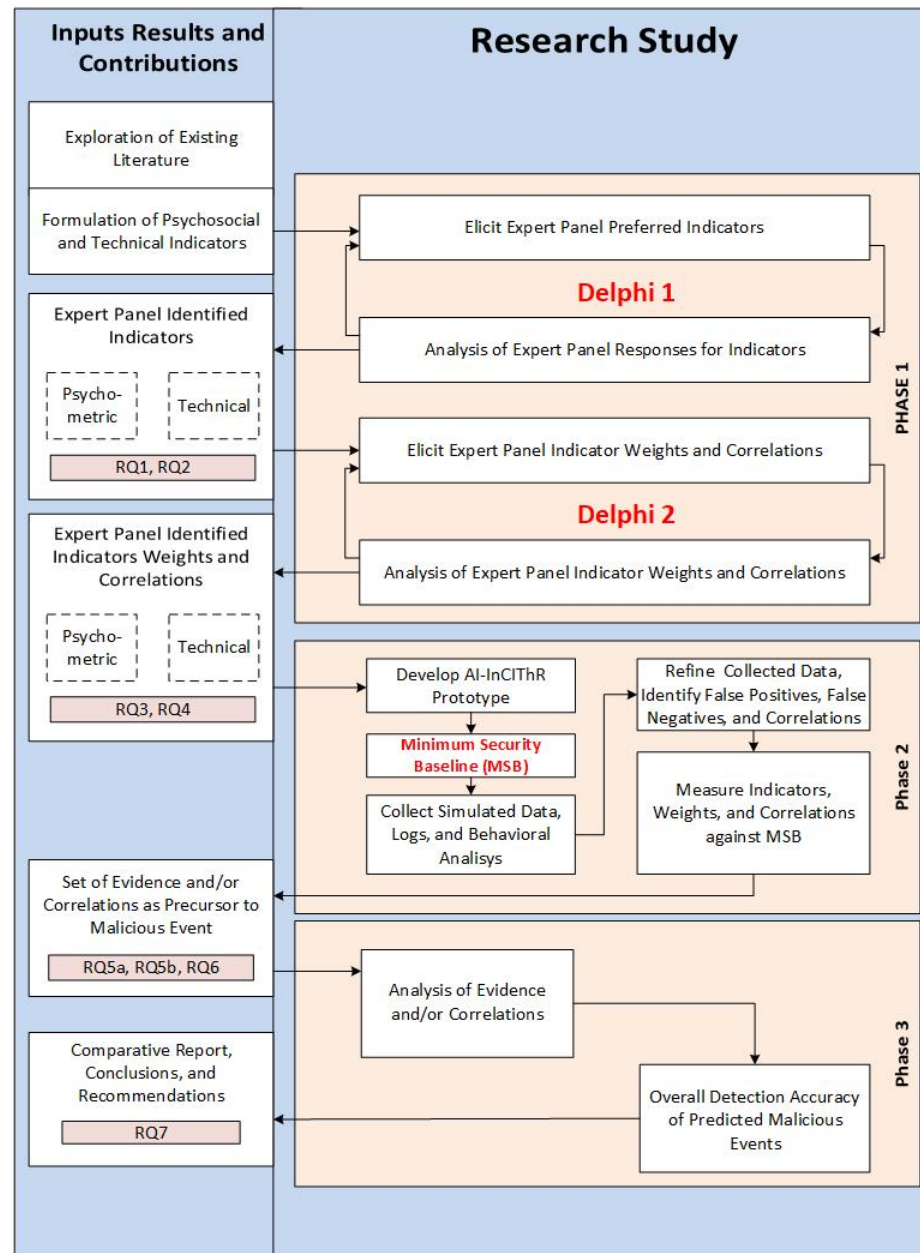


Figure 3. Proposed Overview of the Research Design Process

Instrument Development

Greitzer et al. (2014) recognized the lack of research involving malicious cybersecurity insider threat development of behavioral indicators, as well as, the need for the development of methods to assess the associated insider threat risks (p. 107). Moreover, Greitzer et al. (2010) cautioned, “Predictive approaches cannot be validated a priori; false accusations may harm the career of the accused; and collection/monitoring of certain types of data may adversely affect the employee morale” (p. 1100).

Claycomb et al. (2013) elucidated, when observing human behavior, often only two types of activities are considered: behavioral (i.e., interpersonal human-to-human), and technical (i.e., human interactions with IT). This leaves room for researchers to identify the correlations between both types of behaviors. Greitzer and Hohimer (2011) reiterated, “defining triggers in terms of observable cyber and psychosocial indicators and higher-level aggregated patterns of these behaviors is a major challenge, but also a critical ingredient of a predictive methodology” (p. 43). Early and Stott III (2015) argued the need to identify intelligently, as well as, autonomously, in addition to pinpointing innocuous or unnoticed security event attributes to allow security personnel to remediate preemptively physical, as well as, informational, risks before a security event occurs (p. 1). The White House (2010) issued the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, and one of its main objectives is described as:

General Responsibilities of Departments and Agencies: #2. “Establish an integrated capability to monitor and audit information for insider threat detection and mitigation. Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the

Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) gathering information for a centralized analysis, reporting and response capability.” (The White House, 2010, p. 2)

Many insider threat programs in both the Federal Government and in the private sector focus on technological tools that monitor network traffic and online activity, paying attention only to specific individuals who exhibit suspicious behavior (INSA, 2013). The ease in which end-users are able to transition from personal online accounts to professional networks exacerbates the need to ensure such measures are not tied to malicious cybersecurity insider threat activity.

This study evaluated simulated user activity against a set of indicators which were identified from previously validated research (Oceja, Ambrona, Lopez-Perez, Salgado, & Villegas, 2010). This identified set of both technical and psychometric indicators was then validated by the Delphi technique expert panel selection, with a Web-based survey tool as provided in Appendices C and D. Indicators and indicator groupings validated in the first round then go through a second round of Delphi technique for the expert panel weight assignment of the indicators and expert validated correlations. Once the expert panel validated, grouped, correlated, and assigned weights to the indicators, the final list of indicators was applied to the proof-of-concept prototype, and initial testing began. Table 26 outlines the indicator categories and descriptions that were presented to SMEs through the online survey tool.

SME Data Collection

For Phase 1, this study was conducted using the Delphi technique to collect data from the expert panel. The expert panel consisted of SMEs that are experts in the field of cybersecurity monitoring and response. According to Skulmoski, Hartman, and Krahn (2007), the Delphi technique expert panel can range anywhere from 11 to 345 participants. Skinner, Nelson, Chin, and Land (2015) noted that typical expert panel sizes range anywhere from 10 to 30 SMEs. This research study intended to select 30 SMEs for the expert panel and attempted to have the same SMEs participate in both Delphi 1 and Delphi 2 during Phase 1. This research study accepted cybersecurity certifications and academic degrees as credentials for expert panelists, and intended to solicit the expert advice of SMEs from industry, academia, and the federal government for each iteration of the survey and subsequent rounds if necessary. SMEs that possessed the required credentials were contacted through either direct email or the use of LinkedIn social media Website. SMEs recommended by the Dissertation committee, who possess the required credentials were also accepted. The SMEs expert opinion was collected, as well as, the SMEs demographic information identifying gender, age group, education level, role within the organization, and industry worked in.

Phase 1 – Expert Panel Elicitation

To establish Phase 1, an Institutional Review Board (IRB) approval letter was obtained, as seen in Appendix A. Therefore, Phase 1 of this developmental research elicited industry experts' opinions using the Delphi technique to identify technical and psychometric cybersecurity indicators for measuring malicious cybersecurity insider threat activity (Ramim & Lichvar, 2014). As seen in Figure 3, Phase 1 consisted of two iterations of the Delphi technique, namely, Delphi 1 and Delphi 2, with each Delphi

iteration consisting of multiple rounds. Quantitative and qualitative data for Phase 1 were collected using SurveyMonkey electronic surveys to gather the expert opinions of 30 SMEs.

During Phase 1, Step 1, the SMEs were emailed the Delphi 1, SurveyMonkey electronic survey seen in Appendix C. For each survey item/indicator, the SMEs were asked to rank the survey item/indicator's order of importance for the detection of malicious cybersecurity insider threat attack; using a seven-point Likert scale ranging from (1) "not at all important" to (7) as "extremely important". Once the SMEs consensus was achieved, meaning all the SME's were in agreement, in regard to the SME validated cybersecurity indicators, from all proposed important cybersecurity indicators, the first specific goal was met and RQ1 was addressed.

For Phase 1, Step 2, using the same SurveyMonkey electronic survey, the SMEs were presented with cybersecurity indicator categories as seen in Table 26, and asked to rate the cybersecurity indicator categories by the cybersecurity indicator categories importance in detecting insider threats; this was accomplished using a seven-point Likert scale ranging from (1) "not at all important" to (7) as "extremely important". Once the SMEs consensus was achieved in regard to the cybersecurity indicator categories, the second specific goal was met and RQ2 was addressed. Table 26 outlines the proposed technical and psychometric indicators and indicator categories of the Phase 1, Delphi 1 tentative survey instrument which require SME's input for validation.

Table 26

Indicators Used in Phase I Tentative Survey Instrument

Indicator Category	Indicator Number	Description	Author(s)
Technical: Unauthorized Logon Activity	LG1	Employee logs on to different PC's without proper authorization	Creasy & Glover, 2015; Verizon, 2010
	LG2	Employee logs on after-hours without proper authorization	Creasy & Glover, 2015; Verizon, 2010
	LG3	Employee logs on after-hours more than 30% of the time (9 out of 30 days) without proper authorization	Creasy & Glover, 2015; Verizon, 2010
Technical: Removable Media Device Connection Activity	MC1	Employee connects a removable media device to an organizational PC	Creasy & Glover, 2015; Verizon, 2010
	MC2	Employee disconnects a removable media device from an organizational PC	Creasy & Glover, 2015; Verizon, 2010
Technical: Removable Media Device Connection Activity	MC3	Employee disconnects a removable media device after a PC shutdown	Creasy & Glover, 2015; Verizon, 2010
	MC4	Employee uses (connect/disconnect) a removable media device more than 3 times in one day	Creasy & Glover, 2015; Verizon, 2010
Technical: Removable Media Device File Activity (Open, Write, Copy, Delete) Activity	MF1	Employee opens a file from a removable media device on an organizational PC	Creasy & Glover, 2015; Verizon, 2010

Table 26

Indicators Used in Phase 1 Tentative Survey Instrument (Cont.)

Indicator Category	Indicator Number	Description	Author(s)
Technical: Removable Media Device File Activity (Open, Write, Copy, Delete) Activity	MF2	Employee writes a file to a removable media device	Creasy & Glover, 2015; Verizon, 2010
	MF3	Employee copies a file to a removable media device	Creasy & Glover, 2015; Verizon, 2010
	MF4	Employee copies a file more than 3 times in one day to a removable media device	Creasy & Glover, 2015; Verizon, 2010
	MF5	Employee deletes a file from a removable media device	Creasy & Glover, 2015; Verizon, 2010
Technical: HTTP/Online Activity	HT1	Employee visits an external HTTP site	Creasy & Glover, 2015; Verizon, 2010
	HT2	Employee uploads a file to an external HTTP site	Creasy & Glover, 2015; Verizon, 2010
	HT3	Employee uploads a file to an external HTTP site more than 3 times in one day	Creasy & Glover, 2015; Verizon, 2010
	HT4	Employee downloads a file from an external HTTP site	Creasy & Glover, 2015; Verizon, 2010
	HT5	Employee downloads a file from an external HTTP site more than 3 times in one day	Creasy & Glover, 2015; Verizon, 2010
	HT6	Employee visits an external HTTP site with risky words identified in the organizational word content filtering technology	Creasy & Glover, 2015; Verizon, 2010
Technical: Email Activity	EM1	Employee sends an email with an attachment to an external domain	Creasy & Glover, 2015; Verizon, 2010
	EM2	Employee sends more than 5 emails with an attachment to an external domain	Creasy & Glover, 2015; Verizon, 2010

Table 26

Indicators Used in Phase 1 Tentative Survey Instrument (Cont.)

Indicator Category	Indicator Number	Description	Author(s)
	EM3	Employee receives an email with an attachment from an external domain	Creasy & Glover, 2015; Verizon, 2010
	EM4	Employee receives more than 5 emails with an attachment, from an external domain in one day	Creasy & Glover, 2015; Verizon, 2010
	EM5	Employee sends an internal email with risky words identified in the organizational word content filtering technology	Creasy & Glover, 2015; Verizon, 2010
	EM6	Employee receives an internal email with risky words identified in the organizational word content filtering technology	Creasy & Glover, 2015; Verizon, 2010
	EM7	Employee receives an external email with risky word identified in the organizational word content filtering technology	Creasy & Glover, 2015; Verizon, 2010
	EM8	Employee sends an external email with risky words identified in the organizational word content filtering technology	Creasy & Glover, 2015; Verizon, 2010
Technical: Unauthorized File (Decoy/Honeypot) Access	DF1	Employee accesses a decoy file or honeypot without proper authorization	Creasy & Glover, 2015; Verizon, 2010
	DF2	A PC accesses a decoy file or honeypot without proper authorization	Creasy & Glover, 2015; Verizon, 2010
Psychometric: Openness	PS1	Openness - Personality Traits: Imagination, feelings, actions, ideas	Barrick & Mount, 2010; Judge & Bono, 2000
	PS1A	Low score on Openness: The employee practical conventional, prefers routine, pragmatic, data driven	Barrick & Mount, 2010; Judge & Bono, 2000

Table 26

Indicators Used in Phase 1 Tentative Survey Instrument (Cont.)

Indicator Category	Indicator Number	Description	Author(s)
	PS1B	High Score on Openness: The employee is curious, independent, creative, receptive	Barrick & Mount, 2010; Judge & Bono, 2000
Psychometric: Conscientiousness	PS2	Conscientiousness – Personality Traits: Competence, self-discipline, thoughtfulness, goal driven	Barrick & Mount, 2010; Judge & Bono, 2000
Psychometric: Conscientiousness	PS2A	Low score on conscientiousness: The employee is impulsive, careless, disorganized	Barrick & Mount, 2010; Judge & Bono, 2000
Psychometric: Conscientiousness	PS2B	High score on conscientiousness: The employee is persistent, driven, hardworking, dependable, organized	Barrick & Mount, 2010; Judge & Bono, 2000
Psychometric: Extroversion	PS3	Extroversion – Personality Traits: Sociability, assertiveness, emotional expression	Barrick & Mount, 2010; Judge & Bono, 2000
	PS3A	Low score on Extroversion: The employee is quiet, reserved, withdrawn, reflective	Barrick & Mount, 2010; Judge & Bono, 2000
	PS3B	High score on Extroversion: The employee is outgoing, warm, seeks adventure	Barrick & Mount, 2010; Judge & Bono, 2000
Psychometric: Extroversion	PS3	Extroversion – Personality Traits: Sociability, assertiveness, emotional expression	Barrick & Mount, 2010; Judge & Bono, 2000
	PS3A	Low score on Extroversion: The employee is quiet, reserved, withdrawn, reflective	Barrick & Mount, 2010; Judge & Bono, 2000
	PS3B	High score on Extroversion: The employee is outgoing, warm, seeks adventure	Barrick & Mount, 2010; Judge & Bono, 2000

Table 26

Indicators Used in Phase 1 Tentative Survey Instrument (Cont.)

Indicator Category	Indicator Number	Description	Author(s)
Psychometric: Agreeableness	PS4	Agreeableness - Personality Traits: The employee is cooperative, trustworthy, good-natured	Barrick & Mount, 2010; Judge & Bono, 2000
	PS4A	Low score on Agreeableness: The employee is critical, uncooperative, suspicious, competitive, challenging	Barrick & Mount, 2010; Judge & Bono, 2000
	PS4B	High score on Agreeableness: The employee is helpful, trusting, empathetic, cooperative	Barrick & Mount, 2010; Judge & Bono, 2000
Psychometric: Neuroticism	PS5	Neuroticism – Personality Traits: The employee has a tendency towards negative emotions	Barrick & Mount, 2010; Judge & Bono, 2000
	PS5A	Low score on Neuroticism: The employee is calm, even-tempered, secure	Barrick & Mount, 2010; Judge & Bono, 2000
	PS5B	High score on Neuroticism: The employee is anxious, unhappy, prone to negative emotions	Barrick & Mount, 2010; Judge & Bono, 2000

Once Phase 1, Steps 1 and 2 were completed, processing of the data collected occurred, identifying the SME selected top 10 cybersecurity indicators and indicator categories. During Phase 1, Step 3, the SMEs were emailed the Delphi 2, SurveyMonkey electronic survey as seen in Appendix D, prepopulated with data collected during Phase 1, Steps 1 and 2. Using the Delphi 2 electronic survey, the SMEs were asked to assign weights to the top 10 cybersecurity indicators, using a sliding scale from 1 to 100. When the SMEs reached a consensus on the validated indicator weights, the third specific goal was met and RQ3 was addressed.

Technical: Unauthorized Logon Activity	Technical: Email Activity
LG1: Employee logs on to different PC's without proper authorization	EM1: Employee sends an email with an attachment to an external domain
LG2: Employee logs on after-hours without proper authorization	EM2: Employee sends more than 5 emails with an attachment to an external domain
LG3: Employee logs on after-hours more than 30% of the time (9 out of 30 days) without proper authorization	EM3: Employee receives an email with an attachment from an external domain
Technical: Removable Media Device Connection Activity	EM4: Employee receives more than 5 emails with an attachment, from an external domain in one day
MC1: Employee connects a removable media device to an organizational PC	EM5: Employee sends an internal email with risky words identified in the organizational word content filtering technology
MC2: Employee disconnects a removable media device from an organizational PC	EM6: Employee receives an internal email with risky words identified in the organizational word content filtering technology
MC3: Employee disconnects a removable media device after a PC shutdown	EM7: Employee receives an external email with risky word identified in the organizational word content filtering technology
MC4: Employee uses (connect/disconnect) a removable media device more than 3 times in one day	EM8: Employee sends an external email with risky words identified in the organizational word content filtering technology
Technical: Removable Media Device File Activity (Open, Write, Copy, Delete) Activity	Technical: HTTP/Online Activity
MF1: Employee opens a file from a removable media device on an organizational PC	HT1: Employee visits an external HTTP site
MF2: Employee writes a file to a removable media device	HT2: Employee uploads a file to an external HTTP site
MF3: Employee copies a file to a removable media device	HT3: Employee uploads a file to an external HTTP site more than 3 times in one day
MF4: Employee copies a file more than 3 times in one day to a removable media device	HT4: Employee downloads a file from an external HTTP site
MF5: Employee deletes a file from a removable media device	HT5: Employee downloads a file from an external HTTP site more than 3 times in one day
Psychometric: Openness	Technical: Unauthorized File (Decoy/Honeypot) Access
PS1: Openness - Personality Traits: Imagination, feelings, actions, ideas	DF1: Employee accesses a decoy file or honeypot without proper authorization
PS1A: Low score on Openness: The employee practical conventional, prefers routine, pragmatic, data driven	DF2: A PC accesses a decoy file or honeypot without proper authorization
PS1B: High Score on Openness: The employee is curious, independent, creative, receptive	Psychometric: Conscientiousness
Psychometric: Extroversion	PS2: Conscientiousness – Personality Traits: Competence, self-discipline, thoughtfulness, goal driven
PS3:– Personality Traits: Sociability, assertiveness, emotional expression	PS2A: Low score on conscientiousness: The employee is impulsive, careless, disorganized
PS3A: Low score on Extroversion: The employee is quiet, reserved, withdrawn, reflective	PS2B: High score on conscientiousness: The employee is persistent, driven, hardworking, dependable, organized
PS3B: High score on Extroversion: The employee is outgoing, warm, seeks adventure	Psychometric: Agreeableness
Psychometric: Neuroticism	PS4: Agreeableness - Personality Traits: The employee is cooperative, trustworthy, good-natured
PS5: Neuroticism – Personality Traits: The employee has a tendency towards negative emotions	PS4A: Low score on Agreeableness: The employee is critical, uncooperative, suspicious, competitive, challenging
PS5A: Low score on Neuroticism: The employee is calm, even-tempered, secure	PS4B: High score on Agreeableness: The employee is helpful, trusting, empathetic, cooperative
PS5B: High score on Neuroticism: The employee is anxious, unhappy, prone to negative emotions	

Figure 4: Proposed Indicator Correlation Matrix

Phase 1, Step 4, asked the SMEs to identify the most significant indicator relationships using Figure 4 and a series of dropdown menus as seen in Appendix D. When a consensus was reached for the SME identified significant relationships between indicators, the fourth specific goal was met and RQ4 was addressed.

An analysis of the SMEs opinions was performed to identify the SME agreed upon responses for Phase 1, for the purposes of this research study a consensus was achieved when 70% of expert panel were in agreement, as recommended by Sumsion (1998). When the Delphi technique is used, each round of each phase builds on the previously administered survey instrument, until a consensus of SMEs opinions is achieved. The SurveyMonkey electronic surveys were administered to SMEs from academia, government, and industry, for each Delphi iteration and subsequent rounds if necessary.

Due to the nature of the Delphi method building on the previous round and iteration, the SurveyMonkey survey instruments for Delphi 1 and Delphi 2, were subject to change based on the SMEs recommendations and opinions. This study attempted to gather expert opinion from the same SMEs for the duration of the data collection. When a consensus was achieved for all SME identified indicator validation, indicator categories, indicators weights and indicator correlations, the specific goals and RQs addressed, Phase 1 was complete and the study initiated Phase 2.

Phase 2 – Proof-of-Concept Prototype Development

Phase 2, Step 1, of this research study exercised the aforementioned developed and validated technical, as well as, psychometric indicators into the AI-InCyThR proof-of-concept prototype that was used to collect the simulated user activity data.

Additionally, the simulated data were refined to include the identification of false positives and negatives, together with measure indicators.

As previously mentioned, a Minimum Security Baseline (MSB) allows organizations to deploy systems in a more controlled, efficient, and standardized manner (Livingston, 2000). Fuller and Atlasis (2012) explained that:

“In general, a baseline is a well-defined, well-documented version of the solution at some point in its life cycle, and is used as a foundation to support other activities, including measurement.” (p. 2)

From a technical perspective, Santos (2007) identified that the “initial learning mode and anomaly detection within Cisco IDS/IPS devices is performed over a period of 24 hours by default” (p. 137). However, as noted by Spears and Barki (2010), “in the context of compliance, a control must be implemented for two months (60 days) before its performance can be audited” (p. 515).

The thresholds outlined were representative of an organizational security policy which would capture a baseline as the first 60 days of an employee’s activity. Activity that significantly differentiates from the organizational established baselines are flagged and categorized as a potential policy violation. Grouping several violations per user will rate the user as having a higher tendency towards malicious activity. Per each behavior, two time periods were established, (1) the baseline time period (normal behavior, i.e. 60 days), and (2) the at-risk time period or period of interest (behavior over the employee’s tenure). From these two time periods, three intermediate continuous variables were created: the at-risk variable, the change variable, and the baseline variable. For each behavior, two final dichotomous variables were created, one for the at-risk variable, and

one for the change variable. There were two final binary logistic regression models, one that included only the at-risk dichotomous variables, and the other will include only the change variables.

Operationalization of Risky Behavior Indicators

Phase 2, Step 2, of this developmental research study was the operationalization of the variables into indicators for analysis, and perform data investigation using the AI-InCyThR proof-of-concept prototype on simulated user activity data available from CERT/SEI/CMU. The readily available data set simulates an “aggregated collection of logs from host based sensors distributed across all the computer workstations within a large business or government organization over a 500-day period” (Lindauer et al., 2013, p. 81). The simulated data set represents the logon, external media, HTTP, email, and file access activity of over 4100 simulated users. This simulated data set also presents a simulated users demographic within the organization, as well as a static set of personality traits based on the Five Factor Model of personality.

This research study aimed at defining and measuring the relationships between the following indicators for the detection of malicious cybersecurity insider threat:

Logon – Malicious activity will be defined as the number of days in the time period of interest that a user logs in after hours.

1. Create three continuous variables called “Days_AH_Login_B”(After-Hours; baseline), “Days_AH_Login_C” (% change from baseline), and “Days_AH_Login_R” (at-risk) and will run descriptives to aid in the dichotimization of these variables, including mean, median, skewness, kurtosis, and the frequency distribution.

2. From these descriptive analysis results provide the at-risk and change variable will be dichotomized based on a predetermined cut off. The variables will be called, “AH_Login_R”, and “AH_Login_C”. The cut-off will be chosen such that there is a sufficient number of users in each group. Prior to examining the descriptive data, a reasonable cut off for “AH_Login_R” is at least 30% of the days login after hours (or nine out of 30 days). A reasonable cut off for “AH_Login_C” is at least 30% above baseline use.

External Device – The number of days in the period of interest of which a user connects an external device three or more times in one day.

1. Create three continuous variables called “Days_ED_B”(External Device; baseline), “Days_ED_C” (% change from baseline), “Days_ED_R” (at-risk) and will run full descriptive analysis.
2. From these descriptive analysis results provide the at-risk and change variables will be dichotomized based on a chosen cut off. The variables will be called, “ED_R” and “ED_C”. The cut-off will be chosen such that there is a sufficient number of users in each group. Prior to examining the descriptive data a reasonable cut off for “ED_R” is at least one day where the user used an external device more than three times in the day. A reasonable cut-off for the change variable is having at least one more day external device usage above baseline.

HTTP – Two types of variables will be created, (1) the number of days in the period of interest that the user exceeding either three uploads or three downloads to an external HTTP site per day; (2) the number of days in the period of interest that the user visited an HTTP landing page that contained a “risky” word. The risky word will be identified

using word content filtering, and compared to the identified words listed in the keyword dictionary as outlined in Table 27, and will be flagged, as well as, categorized as a policy violation per the individual employee.

1. Created three continuous variables called “Days_HTTP_B” (http; baseline), “Days_HTTP_C” (% change from baseline), “Days_HTTP_R” (at-risk) and ran full descriptive analysis.
2. From these descriptive analysis results, the at-risk and change variables were dichotomized based on a chosen cut off. The variables were called, “HTTP_R”, “HTTP_C”. The cut-off was chosen such that there was a sufficient number of users in each group. Prior to examining the descriptive data, a reasonable cut off for “HTTP_R” was at least one day where the user used an external device more than three times in the day. A reasonable cut-off for the change variable was having at least one more day of questionable HTTP activity above baseline.
3. For word content filtering a dichotomous variable were created, called “HTTP_RW” (HTTP; Risky Word).
4. A composite four level categorical variable was created to capture both the dichotomous HTTP_R variable and the HTTP_RW variables.
 - a. (0) = Neither HTTP_R or HTTP_RW
 - b. (1) = HTTP_R Positive and HTTP_RW Negative
 - c. (2) = HTTP_R Negative and HTTP_RW Positive
 - d. (3) = Both HTTP_R and HTTP_RW are Positive

Email – Two types of variables were created, (1) the number of days in the period of interest in which user exceeded sending 5 emails with attachments to an external email

address per day (not in the simulated *@dtaa.com domain); (2) the number of days in the period of interest in which the user sent or received an email that contained a “risky” word. The risky word was identified using word content filtering, compared to the identified words listed in the keyword dictionary, and was flagged as well as categorized as a policy violation per the individual user.

1. Created three continuous variables called “Days_Email_B”(email; baseline) , “Days_Email_C” (% change from baseline), “Days_Email_R” (at-risk) and ran full descriptive analysis.
2. From these descriptive analysis results, the at-risk and change variables were dichotomized based on a chosen cut off. The variables were called, “Email_R” , “Email_C”. The cut-off was chosen such that there was a sufficient number of users in each group. Prior to examining the descriptive data a reasonable cut off for “Email_R” was at least one day where the user sent an email with attachment to an external domain more than five times in the day. A reasonable cut-off for the change variable was having at least one more day of questionable email activity above baseline.
3. For word content filtering a dichotomous variable was created, called “Email_RW” (Email; Risky Word).
4. A composite four level categorical variable was created to capture both the dichotomous Email_R variable and the Email_RW variables.
 - a. (0) = Neither Email_R or Email_RW
 - b. (1) = Email_R Positive and Email_RW Negative
 - c. (2) = Email_R Negative and Email_RW Positive

d. (3) = Both Email_R and Email_RW are Positive

File Access – The number of days in the period of interest of which a user copies a file to an external device three or more times in the day.

1. Created three continuous variables called “Days_FA_B”(File Access; baseline) , “Days_FA_C” (% change from baseline), “Days_FA_R” (at-risk) and ran full descriptive analysis.
2. From these descriptive analysis results, the at-risk and change variables were dichotomized based on a chosen cut off. The variables were called, “FA_R”, “FA_C”. The cut-off was chosen such that there was a sufficient number of users in each group. Prior to examining the descriptive data a reasonable cut off for “FA_R” was at least one day where the user copied a file to an external device more than three times in the day. A reasonable cut-off for the change variable was having at least one more day file copy to external device above baseline.

Demographic – This table contains an employee demographics across the organization. This information may be useful for later data exploration and for determining if user role may influence tendency towards malicious actors. This information can be weighted and correlated with user actions in determining a user propensity towards malicious activity. Specifically, does the users role (e.g. IT Staffer, Engineer, etc.) moderate the relationship between the risky behaviors (the predictors) and the malicious use (the dependent variable).

Decoy File – The total number of decoy files that a user access’s and performs and activity (HTTP, Email, Copy) during the period of interest.

1. Created one continuous variable “Number_Decoy_R”, and ran full descriptive analysis.
2. From these descriptive analysis results, the at-risk variable were dichotomized based on a chosen cut off. The variable was called “Decoy_R”. Prior to examining the descriptive data a reasonable cut off for “Decoy_R” was at least one file, where the user accessed a decoy file.

This table includes a list of files that can be used as decoys/honeypot to determine which computer accessed the file. Employee and pc relationships can be used in the weighting of a user’s propensity towards malicious activity.

Psychometric – These are five continuous indicators which were used as predictors for malicious use. The psychometric scale rates employees on a numerical scale. Depending on where an employee lands on the scale, per personality trait being assessed, Openness, Conscientiousness, Extraversion, Agreeableness, or Neuroticism. This information was included in a regression model to predict a user’s propensity towards malicious activity.

1. The dataset includes five continuous indicators for each user: “Psychometric_O”, “Psychometric_C”, “Psychometric_E”, “Psychometric_A”, “Psychometric_N.” For each indicator, full descriptives were run, including the mean, median, mode, and standard deviation, skewness, and kurtosis, and frequency distribution
2. From these descriptives, each variable may have been dichotomized based on a median split.

Total Risk Score – A total risk score was created which encompasses the total count of risky technical and psychometric indicators per user using bivariate logistic

regression to predict a malicious user, creating a baseline and change in total risk score.

1. Created two continuous indicators “Total_B”, “Total_C”, and ran full descriptive analysis.
2. From these descriptive analysis results, each indicator may have been dichotomized based on a median split per each employee.

In continuation, Step 3, of Phase 2 of this developmental research study operationalized these modeling approaches throughout the data analysis process, refining the collected data to identify possible false positives or false negatives. In addressing RQ5a, the result provided for each predictor the prevalence of false positive. A crosstab was produced of each bivariate technical predictor and the dichotomous malicious user outcome variable. A false positive was defined as when the technical predictor is not risky and the malicious user indicator indicated a malicious user.

In addressing RQ5b, the result was for each predictor the prevalence of false negatives. A crosstab was produced of each bivariate technical predictor and the dichotomous malicious user outcome indicator. A false negative was defined as when the technical predictor is risky and the malicious user indicators indicated a non-malicious user. Once this analysis has been achieved with the AI-InCyThR proof-of-concept prototype, the fifth specific goal was met and RQ5a and RQ5b was addressed.

According to Carson (1986), “one of the main problems facing the simulation modeler is gaining the user’s or client’s acceptance of model accuracy” (p. 74). To assist with model verification, validation, and credibility, Caron (1986) identified the distinction between verification, validation, and credibility, which are needed in building

an accurate model that is convincing to the end-users, and an accurate representation of the real system and be used in the decision-making process (p. 74).

- Verification: The process in identifying whether the model is performing as it was designed
- Validation: The process where both the modeler and end-user determine how accurately the model represents reality.
- Credibility: A model which is accepted by the client and is used as an aid in the decision-making process (Carson, 1986)

This developmental research study incorporated these techniques throughout the prototype development process, in order to maintain model accuracy for the particular objectives of this research study (Law, 2009).

Phase 2, Step 4, of this developmental research study measures “both the correlation function and the mutual information measure correlations within one sequence known as ‘autocorrelations,’ or between two sequences known as ‘cross-correlations,’ within the data” (Herzel & Große, 1995, p. 519), allowing for the detection of all dependences. This assisted in addressing RQ6, and identifying which activity indicators were identified the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity. The results of this analysis was a bivariate and multivariate logistic regression to identify the relationship (odds ratio) between an indicator and a malicious user. For example, the bivariate logistic regression will give an odds ratio that indicates how much more likely the risky group is likely to be a malicious user, compared to the non-risky group. The multi-variate logistic regression gives the odds ratio for each predictor adjusting for other predictors in the model.

In the course of Phase 1, the expert panel completed a two-stage Delphi technique to identify the significant indicators, indicator relationships, and indicator weights which were measured to identify “the strength of association between a pair of data vectors” (Shimodaira, 2016, p. 126). Linear regression models were run on the data to determine indicator correlations. Once this stage was completed, a set of evidence and/or correlations as precursors to malicious cybersecurity insider threat events were produced and the sixth specific goal was met, as well as, RQ6 was addressed.

Phase 3 – Analysis of Evidence Against MSB

During Phase 3 of this developmental research study an analysis of the collected evidence and/or correlations against the previously identified MSB was performed. One of the main objectives of this research study was to develop logistic regression models of malicious cybersecurity insider threat as a function of risky behavior predictors. This was accomplished by first identifying and analyzing bivariate associations among the predictors as well as bivariate association between the predictors and the insider threat outcome. The latter was performed for three reasons, 1) in the event that there was a strong relationship between two predictors (multi-collinearity) the indicator with the stronger bivariate association with insider threat outcome was selected, and the other indicator dropped from the logistic regression model. 2) This provided an association (unadjusted) in which to compare whether the addition of other covariates in the logistic regression model affect the bivariate association of interest. 3) This allowed for the validation of the accuracy of the SME’s predicted association between each risky behavior and insider threat outcome.

The approach for determining bivariate association depends on the scale of the particular predictor and outcome. For bivariate associations with two dichotomous indicators a tetrachoric correlation was obtained. Tetrachoric correlation is applicable when both observed “either-or” variables are dichotomous, as explained by Howell (2010, p. 303).

Statistical Measures of Association

As described above the type of measure of association i.e. correlation was determined based on the scale of the indicators. Gingrich (2004), explained that “methods of correlation summarize the relationship between two variables in a single number called the correlation coefficient” (p. 795). According to Goodwin and Leech (2006), correlation is one of the most commonly used statistical techniques in research. It is understood that the most widely used correlation statistic is the Pearson Product-Moment correlation coefficient (Pearson r) (Danacica, 2017; Goodwin & Leech, 2006). Moreover, Goodwin and Leech (2006) explained:

“The Pearson product-moment correlation coefficient describes the size and direction of linear relationship between two continuous variables (generically represented by X and Y), and range from -1.0 (perfect negative relationship) to +1.0 (perfect positive relationship); if no relationship exists between the two variables, the value of the correlation is zero. The symbol r_{xy} (or r) is used to present the correlation calculated.” (p. 252)

Pearson's r can also be used to describe the association between two dichotomous variables. Rovai, Baker, and Ponton (2013), explained that Pearson r is symmetric, meaning that the same coefficient value is obtained regardless of which variable is the

independent variable or the dependent variable. While the Pearson r values range from $-1 \leq r \leq 1$; Hinkle, Wiersma, and Jurs (2003) noted that the absolute values of Pearson r can be interpreted by the size of the correlation coefficient as shown in Table 27.

Table 27

Correlation Coefficient Interpretation

Size of Correlation	Interpretation
.90 to 1.00 (-.90 to -1.00)	Very high positive (negative) correlation
.70 to .90 (-.70 to -.90)	High positive (negative) correlation
.50 to .70 (-.50 to -.70)	Moderate positive (negative) correlation
.30 to .50 (-.30 to -.50)	Low positive (negative) correlation
.00 to .30 (.00 to -.30)	Little if any correlation

Ordinal Logistic Regression

As noted by Mertler and Vannatta (2013), regression is a statistical tool that allows researchers to investigate the effect of independent variables [IVs] (predictive indicators in this study) on the dependent variable [DV] (p. 298). For example, the effect of an employee's single technical activity (i.e. a predictive indicator) on the employee's predisposition towards malicious insider threat activity (DV) In predictive analysis, multiple Ordinal Logistic Regression (OLR) is applied to measures the effect of two or more IVs (predictive indicators in this study) on one dichotomous DV (Lani, 2018). For example, the effect of an employee's technical activities (IV1) and psychometric rating (IV2) on the employee's predisposition towards malicious insider threat activity (DV). As explained by Mertler and Vannatta (2010), in standard multiple regression all the IV's are

entered concurrently; therefore, the effect of the IV's on the DV is evaluated in terms of what it adds to the prediction of the DV as specified by regression equation (p. 164).

Analysis of the Simulated Data Set

A Pearson's correlation matrix was produced of the predictors as an initial test of multi-collinearity. Correlations $\geq .7$ were suspected as multi-collinear for purposes of a multivariate analysis. A separate correlation matrix with outcome variables will be available. Bivariate ordinal logistic regression were run with malicious user as the outcome and each predictor. This provided unadjusted odds ratios, indicating the amount of risk of being a malicious user as a function of the predictor. For example, an odds ratio of 2.5 for the risky logon variable, means that users identified as having risky logon use, have 2.5 times the odds of being a malicious actor, than those users who do not have risky logon use. The residual probability of being a malicious user was obtained for each model, this being a dichotomous variable. Any user with a probability $> .5$ will be considered a malicious user. A two by two cross tab was calculated on the actual malicious users, versus the model identified malicious users, to look for rates of false positives and false negatives, and other sensitivity analysis.

Ordinal Logistic Regression (OLR) was then performed as the non-linear predictive model that includes all the technical behaviors, and psychometric indicators as IVs, and the employee's predisposition towards malicious insider threat activity as DV. This showed the effect of each predictor after controlling for each predictor in the model. The residual probability of being a malicious user was obtained for each model, this being a dichotomous variable. Any user with a probability $> .5$ was considered a malicious user. A two by two cross tab on the actual malicious users, versus the model

identified malicious users, to look for rates of false positives and false negatives, and other sensitivity analysis. The false positive and false negative rates should be improved since there are more predictors that are correlated with the outcomes.

Bivariate and multivariate analysis were run separately for the at-risk predictors.

Word Content Filtering

The importance of email and Internet use in the workplace has been well documented; organizations allow for limited personal Internet use, including social media, in an effort to reduce an employee's negative affect associated with the workplace, and the employers desire for productivity (Vitak, Crouse, & LaRose, 2011; Garrett & Danziger, 2008). Greitzer et al. (2014) explained that another source of psychosocial data is text written by an employee when sending emails using the organizational email system or a sampling of employee social media use approved by the organization (p. 121). Findings from prior research and case studies suggest the presence of personality predispositions in malicious actors, specifically that there is a significant association between word use and personality traits (Greitzer et al., 2014, p. 121); as well as, according to McCrae (2010) a relationship exists between word use and FFM.

As noted earlier, data mining refers to the process of knowledge discovery in data, content monitoring and filtering allows organizations to address the issue of data crossing organizational network boundaries (Proctor & Mogull, 2006). Tools such as Secure Email Gateways and Secure Web Gateways provide a method in which organizations can filter inbound and outbound email message or URL requests against organizationally defined keyword dictionaries or blacklists and can help protect company assets

(Firstbrook & Wynne, 2015; Orans & Firstbrook, 2015). Greitzer et al. (2014) expanded on the use of commercial tools and the detection of malicious insider threats saying,

With some additional analysis it is possible to use output from network auditing appliances to discover psychosocial factors that suggest increased insider threat risk. Specifically the analysis of text used in email and social media communication may be analyzed to identify associated personality traits or psychosocial risk factors (p. 122).

For the purposes of this research study, a risky keyword dictionary outlined by the DHS National Operations Center (NOC) Media Monitoring Capability (MMC) Desktop Reference Binder (Department of Homeland Security, 2011) was used as the foundation to analyze an employee's inbound and outbound email and HTTP activity. An employee who was determined to have a risky word identified in the risky keyword dictionary in their email or HTTP activity was weighted as having a higher propensity to malicious insider threat activity. This rating contributed to the "Total Risk Score" indicator to assist in the prediction of malicious cybersecurity insider threats. Finally, in Phase 3, a report with conclusions and recommendations was produced, meeting the seventh specific goal and addressing RQ7. Table 28 outlined the risky keyword dictionary by threat type and risky words for analysis as identified by DHS.

Table 28

Risky Keyword Dictionary

Keyword Category	Description	Author(s)
------------------	-------------	-----------

Domestic Security	Assassination, Attack, Domestic security, Drill, Exercise, Cops, Law enforcement, Authorities, Disaster assistance, Disaster management, DNDO (Domestic Nuclear Detection Office), preparedness, National Mitigation, Prevention, Response, Recovery, Dirty bomb, Domestic nuclear detection, Emergency management, Emergency response, First responder, Homeland security, Maritime domain awareness (MDA), National preparedness, Initiative, Hostage, Explosion	Department of Homeland Security (2011)
HAZMAT & Nuclear	Hazmat, Nuclear, Chemical spill, Suspicious package/device, Toxic, National laboratory, Nuclear facility, Nuclear threat, Cloud, Plume, Radiation, Radioactive, Leak, Biological infection (or event), Chemical, Chemical burn, Biological, Epidemic, Hazardous, Hazardous material incident, Industrial spill, Infection, Powder (white), Gas, Spillover, Anthrax, Blister agent, Chemical agent, Exposure, Burn, Nerve agent, Ricin, Sarin, North Korea	Department of Homeland Security (2011)
Health Concern & H1N1	Outbreak, Contamination, Exposure, Virus, Evacuation, Bacteria, Recall, Ebola, Food Poisoning, Foot and Mouth (FMD), H5N1, Avian, Flu, Salmonella, Small Pox, Plague, Human to human, Human to Animal, Influenza, Center for Disease Control (CDC), Drug Administration (FDA), Public Health, Toxic, Agro Terror, Tuberculosis (TB), Agriculture Listeria Symptoms Mutation Resistant, Antiviral, Wave, Pandemic, Infection, Water/air borne, Sick, Swine, Pork, Strain, Quarantine, H1N1, Vaccine, Tamiflu, Norvo Virus, Epidemic, World Health Organization (WHO) (and components), Viral, Hemorrhagic Fever, E. Coli	Department of Homeland Security (2011)
Infrastructure Security	Infrastructure security, Airport, Airplane (and derivatives), Chemical fire, CIKR (Critical Infrastructure & Key Resources), AMTRAK, Collapse, Computer infrastructure, Communications, Infrastructure, Telecommunications, Critical infrastructure, National infrastructure, Metro, WMATA, Subway, BART, MARTA, Port Authority, NBIC (National Biosurveillance Integration, Center), Transportation security, Grid, Power, Smart, Body scanner, Electric, Failure or outage, Black out, Brown out, Port, Dock, Bridge, Cancelled, Delays, Service disruption, Power lines	Department of Homeland Security (2011)

Table 28

Risky Keyword Dictionary (Cont.)

Keyword Category	Description	Author(s)
Southwest Border Violence	La Familia, Reynosa, Nuevo Leon, Narcos, Narco banners (Spanish equivalents), Los Zetas, Shootout, Execution, Gunfight, Trafficking, Kidnap, Calderon, Reyosa, Bust, Tamaulipas, Meth Lab, Drug trade, Illegal immigrants, Smuggling (smugglers), Matamoros, Michoacana, Guzman, Arellano-Felix,	Department of Homeland Security (2011)
Southwest Border Violence	Drug cartel, Violence, Gang, Drug, Narcotics, Cocaine, Marijuana, Heroin, Border, Mexico, Cartel, Southwest, Juarez, Sinaloa, Tijuana, Torreon, Yuma, Tucson, Decapitated, U.S. Consulate, Consular, El Paso, Fort Hancock, San Diego, Ciudad Juarez, Nogales, Sonora, Colombia, Mara salvatrucha, MS13, MS-13, Drug war, Mexican army, Methamphetamine, Cartel de Golfo, Gulf Cartel,	Department of Homeland Security (2011)
Terrorism	Terrorism, Al Qaeda, Terror, Attack, Iraq, Afghanistan, Iran, Pakistan, Agro, Environmental terrorist, Eco terrorism, Conventional weapon, Target, Weapons grade, Dirty bomb, Enriched, Nuclear, Chemical weapon, Biological weapon, Ammonium nitrate, Improvised explosive device, IED (Improvised Explosive Device), Abu Sayyaf, Hamas, FARC (Armed Revolutionary Forces Colombia), IRA (Irish Republican Army), ETA (Euskadi ta Askatasuna), Basque Separatists, Hezbollah, Tamil, Tigers, PLF (Palestine Liberation Front), PLO (Palestine Liberation Organization), Car	Department of Homeland Security (2011)
Weather Emergency	Emergency, Hurricane, Tornado, Twister, Tsunami, Earthquake, Tremor, Flood, Storm, Crest, Temblor, Extreme weather, Forest fire, Brush fire, Ice, Stranded/Stuck, Help, Hail, Wildfire, Tsunami Warning Center, Magnitude, Avalanche, Typhoon, Shelter-in-place, Disaster, Snow, Blizzard, Sleet, Mud slide, Mudslide, Erosion, Power outage, Brown out, Warning, Watch, Lightning, Aid, Relief, Closure, Interstate, Burst, Emergency Broadcast System	Department of Homeland Security (2011)

Table 28

Risky Keyword Dictionary (Cont.)

Keyword Category	Description	Author(s)
Cyber Security	Cyber security, Cybersecurity, cybersecurity, Botnet, DDOS (dedicated denial of service), DOS (Denial of service), Malware, Virus, Trojan, Keylogger, Cyber Command, 2600, Spammer, Phishing, Rootkit, Phreaking, Cain and abel, Brute forcing, Mysql injection, Cyber attack, cyber-attack, cyber attack, Cyber terror, Hacker, China, Conficker, Worm, Scammers, Social media, AA Keylogger, Jobhunting, Jobsearch, Closing Project	Department of Homeland Security (2011)

Population and Sample

With the AI-InCyThR system, synthetic user activity over a 500 day period was analyzed for correlations between the expert panel-identified indicators and any anomalies outside of the MSB, identifying possible malicious user activity. Expert panel responses were recorded in a SurveyMonkey spreadsheet. Anomalies and correlations were recorded within the AI-InCyThR system and presented as correlation visualizations. According to Mertler and Vannatta (2010), one of the reasons for pre-analysis data screening is to ensure the accuracy of the data. As they noted, “the results of any statistical analysis are only as good the data analyzed” (p. 25). Mertler and Vannatta (2010) further elaborated that data must be checked for accuracy, since inaccurate data may cause erroneous conclusions.

Data Analysis

As noted by Seuring and Müller (2008), each round of the Delphi technique must be fully documented in order to conduct Delphi technique data analysis. Hasson, Keeney, and McKenna (2000), explained that it is recommended for Delphi technique studies to show the central tendencies and levels of dispersion for each Delphi round. Levels of

dispersion include standard deviation and the inter-quartile range, while central tendencies include means, medians, and mode (Hasson et al., 2000; Skinner et al., 2015). By computing SMEs responses for Delphi 1 and Delphi 2, the means, or average of the SMEs responses were revealed for each item. As well, in computing the medians, the middle value of the SME responses were revealed. Subsequently, the computed modes reveal the most common of the SME response for each item outlined in the survey instrument, with the standard deviation revealing the level of agreement among the SMEs selections. Accordingly, the interquartile range is a measure of variability that is produced by dividing the responses into quartiles.

The expert panel elicitation and AI-InCyThR system pilot test were the foundation to develop a valid and reliable assessment of precursors to malicious insider threat activity. Additionally, an empirical study using the AI-InCyThR system was conducted using 16 months of simulated user activity. Alias (2015) explained that by using an iterative process, increased instrument validity and reliability can be achieved. With the use of a literature review and an expert panel, this study sought to address RQ1 to identify what the most important cybersecurity indicators are, as validated by the experts. This study sought to address RQ2 by utilizing the literature review and expert panel feedback to establish the indicator categories for the most pertinent indicator categorizations. This research also sought to determine the weight for each expert panel validated indicator, and what are the expert-identified most significant correlations between cybersecurity indicators. This was accomplished through the second-round iterative use of the Delphi technique to address RQ3 and RQ4.

Data Analysis with the Proof-of-Concept Prototype

This research sought to address RQ5a by identifying the prevalence of false positives for each predictor. This was accomplished by producing a crosstab of each bivariate technical predictor and the dichotomous malicious user outcome variable. A false positive was defined as when the technical predictor is not risky and the malicious user variable indicated a malicious user. This research sought to address RQ5b by identifying the prevalence of false negatives for each predictor. This was accomplished by producing a cross tab of each bivariate technical predictor and the dichotomous malicious user outcome variable. A false negative was defined as when the technical predictor is risky and the malicious user variable indicated a non-malicious user.

In addition, the results of RQ5a and RQ5b were false positive and false negative rates obtained from the full logistic regression model that includes all predictors simultaneously. A dichotomous predicted malicious user indicator was obtained from the predicted probabilities that are output from this logistic regression model and compared against the actual malicious user variable in a cross tab. A false positive in this case in when the predicted malicious user is negative (i.e. non-malicious user) but the actual malicious user indicator is positive (i.e. malicious user). A false negative in this case in when the predicted malicious user is positive (i.e. malicious user) but the actual malicious user indicator is positive (i.e. non-malicious user).

This research study aimed to address RQ6 by determining what simulated user activity indicators were identified by the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity. This was accomplished by producing a bivariate and multivariate logistic regression to identify the relationship (odds ratio) between an indicator and a malicious user. For example, the bivariate logistic

regression gave an odds ratio that indicates how much more likely the risky group is likely to be a malicious user, compared to the non-risky group. The multivariate logistic regression gets the odds ratio for each predictor adjusting for other predictors in the model.

The results of RQ7 were the SME identified correlations (DV & each predictor) collected in Delphi 2 and outlined in RQ4 compared against the Pearson's correlations (DV & each predictor) empirically-derived from the insider threat data. In order to understand the degree to which SMEs on average underestimate/overestimate the empirically-derived correlations for each DV/predictor combination, the SME correlations for each DV/predictor combination were averaged and compared against the DV/predictor correlations derived from the insider threat data set. For purposes of discussion, "small", "medium" and "large" differences between SME- and empirically-derived correlations were operationalized as follows: small (0 to +/- 0.10), medium (+/- 0.11 to 0.40), large (> +/- 0.40). Linear and Non-Linear correlations with a significant difference and those with little difference were identified and discussed. The average predictor-outcome correlation score was calculated across the SME's for each predictor-outcome pair and compared against the actual correlations derived from the insider threat data set.

Proof-of-Concept Tool and Simulation

Simulated Data Sample

As noted by Barse, Kvarnstrom, and Johnson (2003), synthetic data is defined as data that is generated by simulated users in a simulated environment, performing

simulated actions or activities. These simulations may include human behaviors, or be altogether an automated process (Barse et al., 2003). When using simulated data, great care must be taken to be certain that the simulated data is a true representation of the types of activity that would be expected in real-world scenarios (Hill & Malone, 2004). This is because, as noted by Hill and Malone (2004), data which is too clean or well-arranged will present misleading results. According to Hauduc et al. (2010), “the quality of simulation results can be significantly affected by errors in the model (typing, inconsistencies, gaps, or conceptual errors) and/or in the underlying model description” (p. 1). Furthermore, Hill and Malone (2004) indicated that “benchmarking the dataset can resolve these issues by ensuring the data is realistic” (p. 968). Benchmarking involves comparing the dataset against a series of problems that are both understood and accepted, which will improve the simulated data’s credibility (Hill & Malone, 2004).

The simulated dataset that was used for this study provided test data representing 500 days of user activity, or roughly a year and a half of simulated user activity, for a simulated large organization. Accordingly, the simulated data was categorized and referred to as indicators based on the type of simulated user activity and preconditioned database table classification.

Pilot-Test Initial System

The pilot test of the initial application analyzed three time sets of user activity and event correlation per employee;

- 1) The initial 60-day period that an employee logged in, this sets the initial user baseline of activity. This time frame was chosen because as noted by Spears and Barki (2010), in the context of regulatory compliance, to adhere to the Sarbanes-

Oxley act of 2002, “a control must be implemented for two months before its performance can be audited” (p. 515);

2) A period-of-interest encompassing the employee’s total period-of-employment.

Review of this timeframe allowed for comparison of baseline behavior and any deviations, either positive or negative, in employee activity and behavior.

3) The timeframe which deviation from baseline activity was observed.

As explained by Collins, Onwuegbuzie, and Sutton (2006), the goal in every study, regardless of research field, “is to obtain data that has one or more of the following characteristics: trustworthiness, credibility, dependability, legitimation, validity, plausibility, applicability, consistency, neutrality, reliability, objectivity, confirmability, and/or transferability” (p. 77). Moreover, Collins et al. (2006), elaborated that “instrument fidelity rationale relates to the steps taken by the researcher to maximize the appropriateness and/or utility of the instruments used in the study” (p. 77). Thus, the main focus of this pilot-test was expert panel instrument fidelity. The following phase of the pilot-test evaluated outcome validity. Collins et al. (2006), iterated that outcome validity assesses the “meaning of scores and intended and unintended consequences of using the instrument” (p. 81). Accordingly, proper testing and an expert panel was essential in establishing the fidelity of the AI-InCyThR proof-of-concept prototype, as well as, validate the indicators. The results and observations of this pilot test were evaluated and all adjustments to the indicators of the AI-InCyThR proof-of-concept prototype were completed.

Design and Empirical Study: Revised Proof-of-Concept Prototype

Subsequently, once the initial proof-of-concept prototype was revised, an empirical study was administered using the already developed and validated proof-of-concept prototype. During this phase of the developmental research study, analysis of the simulated user activity over a 60-day period (Spears & Bakari, 2010) was conducted, and the results of this measure documented. Moreover, any recommendations resulting from the data analysis were provided; information regarding the simulated user activity follows.

Table 29

Summary of Research Question (RQ) Triangulation

Research Question (RQ)	Methodology	Data Categorization
RQ1: What are the important cybersecurity indicators validated by the expert panel that can assist in the detection of insider threat activity?	Delphi technique, expert panel elicitation	Extraction of cybersecurity indicators from SME's opinion
RQ2: What are the expert validated cybersecurity indicators categories?	Delphi technique, expert panel elicitation	Extraction of cybersecurity indicator categories from SME's opinion
RQ3: What are the expert-approved-weights for the identified cybersecurity indicators?	Delphi technique, expert panel elicitation	Extraction of cybersecurity indicator weights from SME's opinion
RQ4: What are the expert-identified most significant correlations between cybersecurity indicators?	Delphi technique, expert panel elicitation	Extraction of possible malicious activity based on indicator correlations as identified by SME's opinion
RQ5a: What cybersecurity indicators were identified in experimental settings to have a high rate of false positives as measured by the AI-InCyThR prototype?	Prototype testing, SMB comparison	Results will be the prevalence of false positives for each predictor. A false positive is defined as a technical predictor indicating the user is a malicious user (probability from logistic regression model > 0.50) when, in actuality, the user is not a malicious user.

Table 29

Summary of Research Question (RQ) Triangulation (Cont.)

Research Question (RQ)	Methodology	Data Categorization
RQ5b: What cybersecurity indicators were identified in experimental settings to have a high rate of false negatives as measured by the AI-InCyThR prototype?	Prototype testing, SMB comparison	Results will be the prevalence of false negatives for each predictor. A false negative is defined a technical predictor indicating the user is not a malicious user (probability from logistic regression model ≤ 0.50) when, in actuality, the use is a malicious user.
RQ6: What simulated user activity <i>indicators</i> were identified by the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity?	Prototype output	Results will be bivariate and multivariate ordinal logistic regressions to identify the unadjusted and adjusted relationships (OR), respectively, between the indicators and the malicious user DV.
RQ7: How are the simulated user activity correlations that were identified by the SME's different than those identified by the AI-InCyThR proof-of-concept prototype as significant correlations to identify insider threat activity?	Prototype output and Delphi technique, expert panel elicitation	Results of RQ7 will be the SME identified correlations (DV & each predictor) collected in Delphi 2 and outlined in RQ4 compared against the Pearson's correlations (DV & each predictor) empirically-derived from the insider threat data. In order to understand the degree to which SMEs <i>on average</i> underestimate/overestimate the empirically-derived correlations for each DV/predictor combination, the SME correlations for each DV/predictor combination will be averaged and compared against the DV/predictor correlations derived from the data set.

Reliability and Validity

As noted by Creswell (2012), the reliability and validity of an instrument should, in essence, provide “an accurate assessment of the variables and enable the researcher to draw inferences to a sample or population” (p. 180). Furthermore, Campbell (1957)

detailed the importance of both internal and external validity, and elaborated that internal validity is achieved when the research makes a significant difference in the specific study. As indicated by Ellis and Levy (2009), “internal validity refers to the extent to which its design and the data that it yields allows the researcher to draw accurate conclusions about cause-and-effect and other relationships within the data” (p. 334). Therefore, Salkin (2010) contended that the reliability and validity of a measurement instrument is of the utmost importance, acting as the first screen against inaccurate conclusions on the data being analyzed. Regarding Delphi expert methodology, McFadzean, Ezingard, and Birchall (2011), noted, “the approach ensures that the data collection process is both reliable and valid because it exposes the investigation to differing, and often divergent, opinions and seeks convergence through structured feedback” (p. 108). In their work, Greene, Caracelli, and Graham (1989) stated, “in a complementary mixed-method study, qualitative and quantitative methods are used to measure overlapping but also different facets of a phenomenon, yielding an enriched, elaborated understanding of that phenomenon” (p. 258).

According to Hill and Malone (2004), using simulated data to develop and study diagnostic tools for data analysis is very beneficial. Simulations can be used to suggest an appropriate approximate model, as well as to determine how good an approximation of a given analytic model is (Ignall, Kolesar, & Walker, 1978). Furthermore, Reilly, Staid, Gao, and Guikema (2016) explained that “simulation models are widely used in risk analysis to study the effects if uncertainties on outcomes of interest in complex problems” (p. 1844).

Robinson (1997) explained that a very “significant element of any simulation study is verification and validation (V&V) of the simulation model” (p. 53). According to Robinson (1997), a thorough V&V lays the groundwork on which confidence in the study results can be placed. Davis (1992) noted that *verification* is the process of assuring that the (conceptual) model that has been converted into a computer model meets the developer’s conceptual description and specifications with sufficient accuracy. Validation, according to Carson (1986), consists of the actions taken to assure that the model is fittingly accurate for the functions at hand.

Reliability

The AI-InCyThR was developed to measure the correlations between the fictitious username and an activity as they relate to the established MSB, creating an index of malicious cybersecurity insider threat event precursors. According to Helminen, Halonen, Rankinen, Nissinen, and Rauramaa (1995), the reliability of an index is determined by reproducibility and consistency. Reliability is important in that it indicates the measure of lack of bias, and is indicative of stability and consistency (Sekaran, 2003). By definition, reliability establishes that the “individual scores from an instrument should be nearly the same or staple on repeated administrations of the instrument, they should be free from sources of measurement error, and they should be consistent” (Creswell, 2002, p. 180). Thus, the AI-InCyThR proof-of-concept prototype assessment was validated through testing. As username and event correlations were developed, each correlation was given a score. The overall correlation scores were auto-calculated through the AI-InCyThR algorithm engine.

Validity

Creswell (2002) described *validity* as the researcher's ability to gather significant and relevant generalizations from the survey scores collected. Straub (1989) argued, "that instrument validation at any level can be of considerable help to MIS researchers in substantiating their findings" (p. 162). According to Alias (2015), in general, "measures are valid if they are relevant and clean measures of what the researcher wants to assess" (p. 18). Straub (2015) further elaborated that validity deals with the appropriateness of the method to the research question, which involves the validity of the researcher's interpretation of the data (p. 18). Boudreau, Gefen, and Straub (2001) noted that content validity is another attribute, which is collected and coded. This validity is generally established through literature reviews as well as expert panels. Thus, this study reduced the threat to validity by using input indicators validated by an expert panel that follows the Delphi technique as noted by Ramim and Lichvar (2014).

Resources

In accordance with Nova Southeastern University IRB Policies and Procedures, IRB approval is required to work with human subjects. Access to the cybersecurity industry experts is necessary to follow the Delphi technique expert panel method, as well as, contracting a software developer for developing the AI-InCyThR application. The software prototype was built in a virtual environment using open source tools and operating systems, such as Linux. Fifty \$10 gift cards were given out as an incentive and reward for expert panel participation in the research study. Following the collection of the data, a statistical software program was utilized for data analysis.

Summary

Chapter 3 provided an overview of the methodology for this study. This study was classified as “developmental,” and utilized a mixed-method approach both to weigh and validate the technical and psychosocial indicators to be used in testing the AI-InCyThR proof-of-concept prototype. The AI-InCyThR proof-of-concept prototype was intended to be a means of identifying precursors to malicious cybersecurity insider threat attacks by alerting cybersecurity engineers and managers when certain user activity has exceeded a stated minimum security baseline.

This chapter also discussed the methods with which to address specific research goals and specific research questions. The collection of technical and psychosocial indicators was developed using a literature review, in addition to the feedback received from an expert panel. Moreover, this chapter examined data reliability and validity, data collection procedures, data analysis processes, resources, and the simulated user activity data set.

This chapter outlined a multi-step, three-phased approach towards developing the AI-InCyThR proof-of-concept prototype. After establishing the list of technical and psychosocial indicators derived from the literature, Phase 1 of Delphi method data collection from SMEs proposed and validated the indicators. Step 2 of Phase 1 again relied on the SMEs, now to assign weighted value to the already validated indicators. In Phase 2, the validated and weighted indicators were applied to the AI-InCyThR proof-of-concept prototype and correlated to user activity in comparison to the defined minimum-security baseline, refining the findings and identifying any false positives or false

negatives seen in the data. During Phase 3, analysis of the evidence collected and correlations were hierarchically bundled for visualization, and analyzed for overall detection accuracy.

Chapter 4

Results

Overview

The main goal of this research study was to design, develop, and validate a proof-of-concept prototype for a malicious cybersecurity insider threat alerting system that will assist in the detection and prediction of malicious insider threat activity using human-centric technical activities, as well as, individual employee psychometric rating scales. The previous chapters have introduced the topic, problem, theoretical foundation, and methodology of this study. Chapter 4 will present the results of this study. In Phase 1, the results of two Delphi surveys used to validate indicators, indicator categories, and indicator weights based on an expert panel of SMEs will be presented. In phase two, results of data analysis of a simulated employee activity data set will be presented. Phase three consists of continued analysis of the simulated dataset and comparison to SME opinion.

The main research question this study addressed is: What human-centric technical activity and psychometric indicators are precursors to malicious end-user activity, making those activities rise above a certain threshold to be identified as potential insider threats? The specific research questions (RQ) this study addressed are:

RQ1: What are the important cybersecurity indicators validated by the expert panel that can assist in the detection of insider threat activity?

RQ2: What are the expert-validated cybersecurity indicator categories?

RQ3: What are the expert-approved weights for the identified cybersecurity indicators?

RQ4: What are the expert-identified most significant correlations between cybersecurity indicators?

RQ5a: What cybersecurity indicators were identified in experimental settings to have a high rate of false positives as measured by the AI-InCyThR prototype?

RQ5b: What cybersecurity indicators were identified in experimental settings to have a high rate of false negatives as measured by the AI-InCyThR prototype?

RQ6: What simulated user activity *indicators* were identified by the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity?

RQ7: How are the simulated user activity correlations that were identified by the SMEs different than those identified by the AI-InCyThR proof-of-concept prototype as significant to identify insider threat activity?

Phase 1 - Expert Panel

Data collection in Phase 1 occurred from April 2018 to May 2018 using two Delphi technique survey instruments to collect data from an expert panel. The expert panel consisted of SMEs in the field of cybersecurity and information technology with cybersecurity responsibilities. The goal of this phase was to collect data to validate indicators, indicator categories, and assign indicator weights and correlations. To address RQ1, SMEs were asked to rank user activity indicators on a seven-point Likert scale ranging from (1) *not at all important* to 7 (*extremely important*). The top 10 average highest ranked indicators were chosen as the SME validated indicators. To address RQ2, SMEs were also asked to rank indicator categories in a similar manner. In a second Delphi survey, SMEs were asked to identify what they deemed as important correlations

between indicators as well as assign a weight to the indicators. Data from this survey was used to address RQ3 and RQ4.

Phase 1, Delphi 1 – Data Collection

During Phase 1 of this study, the goal of the SMEs was to identify the most important cybersecurity indicators used to detect the malicious cybersecurity insider threats. Indicators and indicator categories were derived from literature and presented in Chapter 2. The final instrument used for Phase 1 is presented in Appendix C. The SMEs consisted of over 336 cybersecurity and IT professionals with cyber security responsibilities. Individuals in academia and public and private sectors were sourced from LinkedIn social network, all residing in the U.S. SME selection criteria was outlined in Chapter 3. To record the SMEs responses, an email (presented in Appendix C) was sent to the SMEs. This email contained a link to the Web-based survey tool. A total of 46 SMEs completed the Phase 1 survey. No additional rounds of data collection were necessary as qualitative data did not indicate SME desire to add or remove the indicators presented.

Phase 1 – Pre-Analysis Data Screening

Pre-analysis data screening was performed on data collected from the SMEs. Data screening is an important step to ensure accuracy in the data collected as well as to confirm there are no extreme or missing values (Levy & Ellis, 2006; Mertler & Vannatta, 2005). The SMEs responses were collected by way of the SurveyMonkey® Web-based tool, which ensures completeness by impeding incomplete survey submissions. This resulted in none of the surveys submitted being excluded. Through the pre-analysis data screening, no outliers were identified or excluded. Thus, all 46 responses collected were complete and included in the data analysis procedures.

Phase 1, Delphi 1 – Expert Panel Characteristics

There were 46 SMEs who participated in the Delphi 1 survey. The majority of these SMEs were male ($n = 32$, 70%). The largest proportion of SMEs were in the 35-44

age category ($n = 20$, 43%). Slightly more than a third of the SMEs held an IT MS ($n = 16$, 35%). The largest proportion of SMEs were Security Analyst Engineers ($n = 11$, 24%). Half of the SMEs worked in either local, state, or federal government ($n = 23$, 50%). Of those who did not choose one of the offered industry choices and wrote in their answer, industries were: government contractor, non-profit, and technology subject matter expert -issues, opportunities and threats active security clearance, each with an observed frequency of one. The full frequencies and percentages of the SME demographics are presented in Table 30.

Table 30

Frequency Table for SME Demographics

Variable	<i>n</i>	%
Gender		
Female	14	30.43
Male	32	69.57
Age		
25-34	5	10.87
35-44	20	43.48
45-54	13	28.26
55-64	7	15.22
65-74	1	2.17
Education		
High School Diploma	1	2.17
Bachelor's degree	9	19.57
MBA	7	15.22
OJT	6	13.04
PhD	4	8.70
Professional Doctorate	3	6.52

Table 30

Frequency Table for SME Demographics

Variable	<i>n</i>	%
Role		
Academia Researcher	7	15.22
CIO/CISO/CEO/CFO/COO	5	10.87
Cybersecurity Program Management	6	13.04
Security Analyst Engineer	11	23.91
Security Operations Manager	3	6.52
Technical Analyst Engineer	5	10.87
Technical Lead IT Professional	9	19.57
Industry		
Education	7	15.22
Financial Banking	2	4.35
Healthcare	3	6.52
Local State Federal Government	23	50.00
Other please specify	3	6.52
Private Industry/Commercial	8	17.39
Industry—Other (write-in responses)		
Government contractor	1	2.17
Non-profit	1	2.17
Technology SME with ACTIVE Security Clearance	1	2.17
No Answer	43	93.48

Note. Due to rounding errors, percentages may not equal 100%.

Phase 1, Delphi 1 – Data Analysis

In Phase 1, Delphi 1, the data collected via the SurveyMonkey® survey tool was exported to Microsoft Excel for initial analysis and processing. The SME responses to

RQ1 and RQ2 were parsed to identify the count for each indicator and indicator category. To address RQ1, what are the important cybersecurity indicators validated by the expert panel that can assist in the detection of insider threat activity? SMEs were asked to rank cybersecurity indicators in order of importance using a seven-point Likert scale ranging from (1) *not at all important* to (7) *extremely important*. The most important cybersecurity indicators validated by the expert panel were identified by ranking the top ten items by average score. From most important to least important the top ten most important cybersecurity indicators were LG1, LG2, LG3, MC1, HT6, EM8, EM7, EM6, EM5, and PS2A. Table 31 presents means and standard deviations of the importance of these indicators as well as a description of each indicator.

Table 31

Means and Standard Deviations of Importance of Indicators

Indicator Number	Indicator Description	Importance	
		<i>M</i>	<i>SD</i>
LG1	Employee logs on to different PC's without proper authorization	6.2	0.88
LG3	Employee logs on after hours more than 30% of the tenure days without proper authorization	6.1	1.01
LG2	Employee logs on after-hours more than 30% of the time (9 out of 30 days) without proper authorization	6.0	1.26
EM8	Employee sends an external email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	6.0	1.19

Table 31

Means and Standard Deviations of Importance of Indicators (Cont.)

Indicator Number	Indicator Description	Importance	
		<i>M</i>	<i>SD</i>
HT6	Employee visits an external HTTP site with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	5.8	1.05
EM7	Employee receives an external email with risky word identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	5.7	1.38
EM5	Employee sends an internal email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	5.5	1.46
PS2A	Low score on conscientiousness: The employee is impulsive, careless, disorganized	5.5	1.52
EM6	Employee receives an internal email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days).	5.4	1.49
MC1	Employee connects a removable media device to an organizational PC	5.3	1.46

To address RQ2. what are the expert-validated cybersecurity indicator categories? SMEs were asked to rank the importance of indicator categories on a scale of (1) *not important* to (7) *very important*. Table 32 presents the mean importance rating of the top 10 most highly rated indicator categories. Indicator categories identified as most important included technical (unauthorized logon activity, removable media device file activity, and removable media device connection activity, HTTP/online activity, email activity) and psychometric (neuroticism, conscientiousness, openness, agreeableness, extroversion). The most important category rated was technical: unauthorized logon

activity. The lowest ranked most important category was psychometric: extroversion.

Although each of the indicators from these categories were considered important, the majority of indicators individually identified as important were regarding email activity and logon activity.

Table 32

Means and Standard Deviations of Importance of Indicator Categories

Indicator Category		Importance	
		<i>M</i>	<i>SD</i>
Technical	Unauthorized Logon Activity	6.4	0.91
Technical	Removable Media Device File Activity (Open, Write, Copy, Delete) Activity	5.6	1.29
Technical	Removable Media Device Connection Activity	5.4	1.26
Psychometric	Neuroticism	5.1	1.21
Technical	HTTP/Online Activity	4.9	1.39
Technical	Email Activity	4.8	1.33
Psychometric:	Conscientiousness	4.7	1.48
Psychometric:	Openness	4.4	1.45
Psychometric:	Agreeableness	4.4	1.34
Psychometric:	Extroversion	4.2	1.37

Phase 1, Delphi 2 – Data Collection

Over a two-week period, the Phase 1, Delphi 2 survey instrument was sent to the 336 previously identified SMEs and collected 26 responses for an 8% response rate. The SMEs were asked to assign a weight to the indicators as well as identify what they deemed as important correlations between indicators. Data from this survey was used to address RQ3 and RQ4.

Phase 1, Delphi 2 – Pre-Analysis

Pre-analysis data screening did not identify any qualitative SME responses that suggested that indicators needed to be added or removed. The survey was set up to now allow incomplete responses. As such, no incomplete responses were collected.

Phase 1, Delphi 2 – Data Analysis

As previously mentioned, the most important cybersecurity indicators validated by the expert panel were identified by ranking the top ten items by average score. From most important to least important the top ten most important cybersecurity indicators were LG1, LG2, LG3, MC1, HT6, EM8, EM7, EM6, EM5, and PS2A. To address RQ3, what are the expert-approved weights for the identified cybersecurity indicators? SMEs were asked to assign the top 10 indicators weights based on a scale of 1 to 100. The most highly weighted indicator, on average, was LG3 ($M = 81.2$; $SD = 17.3$). The lowest weighted indicator was EM7 ($M = 59.5$, $SD = 2.78$). Table 33 presents the means and standard deviations of these indicator weights.

Table 33

Means and Standard Deviations of Importance of Indicator Weights

Indicator Number	Indicator Description	Weight	
		<i>M</i>	<i>SD</i>
LG3	Employee logs on after hours more than 30% of the tenure days without proper authorization	81.2	17.3
PS2A	Low score on conscientiousness: The employee is impulsive, careless, disorganized	78.6	21.7
LG1	Employee logs on to different PC's without proper authorization	78.3	16.2
EM6	Employee receives an internal email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	77.1	21.3

Table 33

Means and Standard Deviations of Importance of Indicator Weights (Cont.)

Indicator Number	Indicator Description	Weight	
		<i>M</i>	<i>SD</i>
MC1	Employee connects a removable media device to an organizational PC	75.7	20.9
LG2	Employee logs on after-hours more than 30% of the time (9 out of 30 days) without proper authorization	73.0	18.4
EM8	Employee sends an external email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	70.0	24.5
HT6	Employee visits an external HTTP site with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	67.9	24.2
EM5	Employee sends an internal email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	61.6	26.5
EM7	Employee receives an external email with risky word identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	59.5	27.8

To address RQ4, what are the expert-identified most significant correlations between cybersecurity indicators? SMEs were asked to choose important correlations between indicators. The top 10 most frequently identified pairings were retained as significant correlations. Pairings with frequencies less than three were excluded. These results are presented in Table 34.

For correlation number 1, the most frequently identified pairing was between HT5 and HT4. For correlation number 2, the most frequently identified pairing was between EM8 and EM7. For correlation number 3, the most frequently identified pairing was

between HT3 and HT5. For correlation number 4, the most frequently identified pairing was between PS4A and LG3. For correlation number 5, the most frequently identified pairing was between EM8 and EM5. For correlation number 6, the most frequently identified pairing was between HT2 and HT3. For correlation number 7, the most frequently identified pairing was between LG2 and LG3. For correlation number 8, the most frequently identified pairing was between MF3 and HT3. For correlation number 9, the most frequently identified pairing was between PS5A and PS5. For correlation number 10, the most frequently identified pairing was between PS5B and EM8.

Table 34

SME-Identified Correlations

Correlation #	Indicator 1	Indicator 2	Frequency Identified
1	HT5	HT4	5
2	EM8	EM7	4
3	HT3	HT5	4
4	PS4A	LG3	4
5	EM8	EM5	3
6	HT2	HT3	3
7	LG2	LG3	3
8	MF3	HT2	3
9	PS5A	PS5	3
10	PS5B	EM8	3

Phases Two and Three-Analysis of Simulated User Activity

Data analysis for phases two and three occurred from June 2018 to October 2018 using a simulated user activity dataset. The goal of this phase was to analyze data representing simulated user activity that may or may not be malicious. To address RQ5a

and RQ5b, cross-tabulations were created between the indicator categories identified by the SMEs as well as identified by the system to determine the number of false positives and false negatives. To address RQ6, bivariate binary logistic regressions were used to determine what the system as identified as significant predictors of malicious activity, as well as, which of the SME-validated indicators were significantly predictive of malicious activity. To address RQ7, the SME rankings of indicator importance were compared to results of binary logistic regressions.

Phases Two and Three– Data Collection

As noted by Lindauer et al. (2013), while insider threat research is of paramount importance, one of the greatest challenges in this field of research is obtaining suitable data for research, testing, and development. This is due to the fact that insiders are employees of the organization; in order to collect user activity data, organizations must monitor, record, and analyze the behaviors and actions of their own employees. This type of real time employee monitoring raises confidentiality and privacy concerns, making it preferable for researchers to use synthetic data (Glasser & Lindauer, 2013).

The simulated user activity dataset analyzed for this study was obtained from Carnegie Mellon University’s Software Engineering Institute, CERT National Insider Threat Center. The simulated data represents an aggregated “collection of logs from host-based sensors distributed across all the computer workstations within a large business or government organization over a 500-day period” (Glasser & Lindauer, 2013, p. 1).

Phases Two and Three – Pre-Analysis Data Screening

Pre-analysis data screening was used to determine that the data set consisted of 115 million lines of simulated user activity. Simulated user activities ranged from logon/logoff behavior, email patterns, HTTP visits, external media/USB usage, file copies or changes, attempted restricted file access, demographics, and psychometric scale

ratings. All but one of the indicator categories presented to the SMEs produced reasonable odds ratios and were used in the data analysis of this study. The indicator Decoy File category presented two indicators DF1 and DF2 as seen in Table 33. For DF1, the simulated dataset lacked the employee to PC relationship needed to analyze this indicator. DF2 produced a high false positive rate indicating that 90.07% of PC's produced this activity. As a result, these indicators were dropped from the study and were replaced with EM6 and MC1, the indicators with the next highest mean in the SME identified order of importance. After data screening, the final dataset consisted of 4118 simulated users, with 118 of those users known malicious insider threat actors.

Table 35

Decoy File Indicators

Indicator Number	Indicator Description	Frequency	
		<i>0</i>	<i>1</i>
DF1	An employee accesses a decoy file or honeypot without proper authorization	NA	NA
DF2	A PC accesses a decoy file or honeypot without proper authorization	409	3708

*Phase Two and Three—Data Analysis**Research Questions 5a and 5b*

RQ5a: What cybersecurity indicators were identified in experimental settings to have a high rate of false positives as measured by the AI-InCyThR prototype?

RQ5b: What cybersecurity indicators were identified in experimental settings to have a high rate of false negatives as measured by the AI-InCyThR prototype?

To address this research question, crosstabulations of the categories of each indicator variable (categories: yes, performed activity; no, did not perform activity) identified by the system and the variable malicious user (yes, flagged as actual malicious user; no, not actual malicious user) were generated. Then, the percentages of users who were malicious users and did perform the indicator activity were compared to the percentages of users who were malicious users and did not perform the activity. Table 34 presents the results of these crosstabulations.

For LG4, almost all malicious users did not perform this activity (99.19%). Similarly, only 2.70% of non-malicious users performed this activity. For MC4, almost all non-malicious users did not perform this activity (97.58%). A fair amount of non-malicious users did perform this activity (19.03%). For MF4, all malicious users did not perform this activity (100%). Similarly, only 2.60% of non-malicious users performed this activity. For EM2, almost all non-malicious users did not perform this activity (99.19%). Of the non-malicious users, 5.03% performed this activity. For EM9, the majority of non-malicious users did not perform this activity (96.77%), and the majority of non-malicious users did perform the activity (82.29%). For HT7, the majority of malicious users did not perform this activity (96.77%), and a small amount of non-malicious users did perform this activity (15.25%). For PS1B, three-quarters of malicious users did not perform this activity, while just under a third of non-malicious users did perform this activity (29.03%). For PS3B, a majority of malicious users did not perform this activity (76.61%), and 26.60% of non-malicious users performed this activity. For PS4B, 71.77% of malicious users did not perform this activity, while 25.64% of non-

malicious users did perform this activity. For PS5B, 73.39% of malicious users did not perform this activity, while 27.97% of non-malicious users did perform this activity.

For the system identified indicators, the majority of indicators had a high rate of false negatives (ranging from 71.77% to 100%). EM9 had the highest rate of false positives. LG4 and MF4 had the lowest rate of false positives.

Table 36

Crosstabulation Between System-Identified Indicator Activity and Malicious User

Indicator	Malicious User	
	No (n, sample %; column %)	Yes (n, sample %; column %)
LG4		
No	3885 (94.36%; 97.305)	123 (2.99%; 99.19%)
Yes	108 (2.62%; 2.70%)	1 (0.02%; 0.81%)
MC4		
No	3233 (78.53%; 80.97%)	121 (2.94%; 97.58%)
Yes	760 (18.46%; 19.03%)	3 (0.07% ; 2.42%)
MF4		
No	3889 (94.46%; 97.40%)	124 (3.01%; 100%)
Yes	104 (2.53%; 2.60%)	0 (0.00%; 0.00%)
EM2		
No	3792 (92.11%; 94.97%)	123 (2.99%; 99.19%)
Yes	201 (4.88%; 5.03%)	1 (0.02%; 0.81%)
EM9		
No	707 (17.17%; 17.71%)	120 (2.91%; 96.77%)
Yes	3286 (79.82%; 82.29%)	4 (0.10%; 3.23%)
HT7		
No	3384 (82.20%; 84.75%)	120 (2.91%; 96.77%)
Yes	609 (14.79; 15.25%)	4 (0.10%; 3.23%)
PS1B		
No	2834 (68.84%; 70.97%)	93 (2.26%; 75.00%)
Yes	1159 (28.15; 29.03%)	31 (0.75%; 25.00%)

Table 36

Crosstabulation Between System-Identified Indicator Activity and Malicious User (Cont.)

Indicator	Malicious User	
	No (<i>n</i> , sample %; column %)	Yes (<i>n</i> , sample %; column %)
PS3B		
No	2923 (71.00; 73.20%)	95 (2.31%; 76.61%)
Yes	1070 (25.99%; 26.80%)	29 (0.70%; 23.39%)
PS4B		
No	2969 (72.12%; 74.36%)	89 (2.16%; 71.77%)
Yes	1024 (24.87%; 25.64%)	35 (0.85%; 28.23%)
PS5B		
No	2876 (69.86%; 72.03%)	91 (2.21%; 73.39%)
Yes	1117 (27.13%; 27.97%)	33 (0.80%; 26.61%)

Next, crosstabulations of the categories of each indicator variable identified by the SMEs and the variable malicious user were generated. Table 37 presents the frequencies and percentages associated with these crosstabulations. For LG1, the majority of malicious users did not perform the activity (71.77%). Of the non-malicious users, 29.18% did perform this activity. For LG2, the majority of malicious users did perform the activity (84.68%). Less than a quarter of non-malicious users performed this activity (22.11%). For LG3, the majority of malicious users did not perform the activity (52.42%). Only 2.48% of non-malicious users performed this activity.

For MC1, almost all malicious users did not perform the activity (96.77%). Less than a quarter of non-malicious users did perform this activity (19.61%). For HT6, the majority of malicious users did not perform the activity (97.58%). No non-malicious user performed this activity (0.00%). For EM8, the majority of malicious users did not perform the activity (98.39%). A sizeable amount of non-malicious users performed this activity (41.97%). For EM7, the majority of malicious users did not perform the activity

(97.58%). The majority of non-malicious performed this activity (64.01%). For EM6, almost all malicious users did not perform the activity (99.19%). Slightly less than half of non-malicious users performed this activity (48.79%). For EM5, almost all malicious users did not perform the activity (99.19%). Almost a third of non-malicious users performed this activity (30.15%). For PS2A, the majority of malicious users did not perform the activity (70.16%). Less than a third of non-malicious users performed this activity (27.62%).

Out of the ten indicators, only LG2 correctly identified the malicious user the majority of the time (84.68%). The indicator that correctly identified the malicious user the next highest majority of the time was LG3, at 47.58%. Almost all other indicators had a very high percentage of false negatives. EM8, EM7, and EM6 had the highest percentages of false positives, with 41.96-64.01% of non-malicious users having performed the activity.

Table 37

Crosstabulation Between SME-Identified Indicator Activity and Malicious User

Indicator	Malicious User	
	No (n, sample %; column %)	Yes (n, sample %; column %)
LG1		
No	2828 (68.69%; 70.82%)	89 (2.16%; 71.77%)
Yes	1165 (28.30%; 29.18%)	35 (2.92%; 28.23%)
LG2		
No	3110 (75.54%; 77.89%)	19 (0.46%; 15.32%)
Yes	883 (21.45%; 22.11%)	105 (2.55%; 84.68%)
LG3		
No	3894 (94.58%; 97.52%)	65 (1.58%; 52.42%)
Yes	99 (2.40%; 2.48%)	59 (1.43%; 47.58%)

Table 37

Crosstabulation Between SME-Identified Indicator Activity and Malicious User (Cont.)

Indicator	Malicious User	
	No (<i>n</i> , sample %; column %)	Yes (<i>n</i> , sample %; column %)
MC1		
No	3210 (77.97%; 80.39%)	120 (2.91%; 96.77%)
Yes	783 (19.02%; 19.61%)	4 (0.10%; 3.23%)
HT6		
No	3993 (96.99%; 100%)	121 (2.94%; 97.58%)
Yes	0 (0.00%; 0.00%)	3 (0.07%; 2.42%)
EM8		
No	2317 (56.28%; 58.03%)	122 (2.96%; 98.39%)
Yes	1676 (40.71%; 41.97%)	2 (0.05%; 1.61%)
EM7		
No	1437 (34.90%; 35.99%)	121 (2.94%; 97.58%)
Yes	2556 (62.08%; 64.01%)	3 (0.07%; 2.42%)
EM6		
No	2045 (49.67%; 51.21%)	123 (2.99%; 99.19%)
Yes	1948 (47.32%; 48.79%)	1 (0.02%; 0.81%)
EM5		
No	2789 (67.74%; 69.85%)	123 (2.99%; 99.19%)
Yes	1204 (29.24%; 30.15%)	1 (0.02%; 0.81%)
PS2A		
No	2890 (70.20%; 72.38%)	87 (2.11%; 70.16%)
Yes	1103 (26.79%; 27.62%)	37 (0.90%; 29.84%)

Research Question 6

RQ6: What simulated user activity *indicators* were identified by the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity?

To address this research question, a series of bivariate binary logistic regressions were performed. The binary dependent variable for each regression was malicious user (1 = yes, flagged as actual malicious user, 0 = no, not actual malicious user). The predictor variables were user activity indicators (1 = yes, performed activity, 0 = no, did not perform activity) identified by the system, as well indicators identified by the SMEs.

Then, a multivariate model was specified which included all indicators identified by the SMEs in one model.

The bivariate models involving indicators identified by the system are summarized in Table 38. EM9 was a significant predictor of being a malicious user, $OR = 0.01, p < .001$. The odds of being a malicious user are 0.01 times lower for users who perform this activity when compared to users who do not perform this activity. HT7 was a significant predictor of being a malicious user, $OR = 0.19, p = .001$. The odds of being a malicious user were 0.19 times lower for users who performed this activity when compared to those who do not perform this activity. No other indicator was a significant predictor.

Table 38

*Results of Bivariate Binary Logistic Regression with System-Identified Indicators
Predicting Likelihood of Malicious User*

Indicator	<i>B</i>	<i>SE</i>	OR	<i>p</i>
MC4	-1.23	1.01	0.29	.223
MF4	-14.05	625.2	< .001	.982
EM2	-1.87	1.01	.015	.063
EM9	-4.94	0.51	0.01	< .001***
HT7	-1.69	0.51	0.19	.001**
PS1B	-0.20	0.21	0.82	.331
PS3B	-0.18	0.22	0.83	.399
PS4B	0.13	0.21	1.14	.518
PS5B	-0.07	0.21	0.93	.739

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

The bivariate models involving indicators identified by the SMEs are summarized in Table 39. All indicators were significantly predictive of likelihood of being a malicious user to various amounts except for LG1, HT6, and PS2A. HT6 showed greatly inflated estimates, indicating that results should be treated with caution. Performance of Lg2 and LG3 were predictive of increased chances of being a malicious user, while performance

of the other significant predictors were indicative of a decreased chance of being a malicious user.

Table 39

Results of Bivariate Binary Logistic Regression with SME-Identified Indicators Predicting Likelihood of Malicious User

Indicator	<i>B</i>	<i>SE</i>	OR	<i>p</i>
LG1	-0.05	0.21	0.96	.819
LG2	2.97	0.25	19.46	< .001***
LG3	3.57	0.21	35.70	< .001***
MC1	-1.99	0.51	0.14	< .001***
HT6	34.23	2718231	> 999.99	1.00
EM8	-3.79	0.71	0.02	< .001***
EM7	-4.27	0.58	0.01	< .001***
EM6	-4.76	1.00	0.01	< .001***
EM5	-3.97	1.00	0.02	< .001***
PS2A	0.11	0.20	1.11	.587

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

A multivariate model was then specified with each of the SME-identified indicators. First, multicollinearity between the predictor variables was assessed using tetrachoric correlations. Correlations were considered strong if they were .80 or above and significant (Tabachnick & Fidell, 2014). HT6 had a strong correlation with almost all predictors. There was a strong correlation between LG1 and LG2 (0.84, $p < .001$). There was a strong correlation between LG2 and LG3 (0.99, $p < .001$) and HT6 (1.00, $p = .003$). As such, HT6 and LG2 were removed from the model because there was collinearity with other indicators in the model.

The overall regression model was significant, $\chi^2(9) = 688.73$, $p < .001$. This indicates that at least one of the indicators significantly predicts the likelihood of a user being classified as malicious. As such, the individual indicators were examined. The results of the binary logistic regression are summarized in Table 38.

LG1 was a significant predictor of malicious users, odds ratio (OR) = 2.74, $p < .001$. This indicates that the odds of being a malicious user are 2.74 times higher if the user performs this activity when compared to users who do not perform this activity. LG3 was a significant predictor of malicious users, OR = 58.97, $p < .001$. The odds of being a malicious user are 58.97 times higher if the user performs this activity. MC1 was a significant predictor of malicious users, OR = 0.10, $p < .001$. This indicates that those who performed this activity had 0.10 times lower odds of being a malicious user. EM8 was a significant predictor of malicious users, OR = 0.06, $p = .001$. Those who performed this activity had 0.06 lower odds of being a malicious user. EM7 was a significant predictor of malicious users, OR = 0.01, $p < .001$. Those who performed this activity had 0.01 times lower odds of being a malicious user. EM6 was a significant predictor of malicious users, OR = 0.02, $p < .001$. Those who performed this activity had 0.02 times lower odds of being a malicious user. EM5 and PS2A did not significantly predict changes in the likelihood of being a malicious user.

Table 40

Multivariate Binary Logistic Regression with Indicators Predicting Likelihood of Malicious User

Indicator	<i>B</i>	<i>SE</i>	OR	<i>p</i>
Intercept	-2.53	0.18	-	< .001***
LG1	1.01	0.27	2.74	< .001***
LG3	4.08	0.34	58.97	< .001***
MC1	-2.30	0.59	0.10	< .001***
EM8	-2.83	0.81	0.06	< .001***
EM7	-4.76	0.69	0.01	< .001***
EM6	-3.82	1.07	0.02	< .001***

Table 40

Multivariate Binary Logistic Regression with Indicators Predicting Likelihood of Malicious User (Cont.)

Indicator	<i>B</i>	<i>SE</i>	OR	<i>p</i>
EM5	-1.97	1.02	0.14	.054
PS2A	0.19	0.26	1.21	.454

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Research Question 7

RQ7: How are the simulated user activity correlations that were identified by the SMEs different than those identified by the AI-InCyThR proof-of-concept prototype as significant to identify insider threat activity?

To address this research question, the average importance of each SME-identified indicator was compared towards their actual significance and OR as reported by bivariate logistic regressions (see Table 37 for the bivariate logistic regressions). Table 39 presents the SME rankings and the ORs and actual significance.

On average, SMEs ranked LG1 the highest in importance. However, when assessed statistically, this was not an actual significant predictor of malicious users. LG3 was ranked the second highest in importance. When assessed statistically, this was a significant predictor with a high OR. LG2 was ranked third. When assessed statistically, this was a significant predictor with a high OR that was below the OR of LG3. EM8 was ranked fourth. This was a significant predictor with a very small OR, indicating that the activity predicts lower odds of being a malicious user. HT6 showed inflated estimates, indicating that results were not reliable, and thus was not reported here. EM 7 was ranked sixth. This was a significant predictor with an OR similar to EM8, indicating lower odds of being a malicious user. EM5 was ranked seventh. This was a significant predictor with a OR similar to EM8 and EM7, indicating lower odds of being a malicious user. PS2A

was ranked eighth. This was not a significant predictor. EM6 was ranked ninth, this was a significant predictor with a small OR, indicating lower odds of being a malicious user.

Finally, MC1 was ranked 10th most important. This was a significant predictor with a low OR, indicating lower odds of being a malicious user.

Table 41

Indicator SME-Identified Average Importance, OR, and Significance of Indicators

Indicator Number	Indicator Description	Importance		OR	<i>p</i>
		<i>M</i>	<i>SD</i>		
LG1	Employee logs on to different PC's without proper authorization	6.2	0.88	0.96	.819
LG3	Employee logs on after hours more than 30% of the tenure days without proper authorization	6.1	1.01	35.70	< .001***
LG2	Employee logs on after-hours more than 30% of the time (9 out or 30 days) without proper authorization	6.0	1.26	19.46	< .001***
EM8	Employee sends an external email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out or 30 days)	6.0	1.19	0.02	< .001***
HT6†	Employee visits an eternal HTTP site with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out or 30 days)	5.8	1.05	-	-
EM7	Employee receives an external email with risky word identified in the organizational word content filtering technology more than 30% of the time (9 out or 30 days)	5.7	1.38	0.01	< .001***

Table 41

Indicator SME-Identified Average Importance, OR, and Significance of Indicators (Cont.)

Indicator Number	Indicator Description	Importance		OR	<i>p</i>
		<i>M</i>	<i>SD</i>		
EM5	Employee sends an internal email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days)	5.5	1.46	0.02	<.001***
PS2A	Low score on conscientiousness: The employee is impulsive, careless, disorganized	5.5	1.52	1.11	.587
EM6	Employee receives an internal email with risky words identified in the organizational word content filtering technology more than 30% of the time (9 out of 30 days).	5.4	1.49	0.01	< .001***
MC1	Employee connects a removable media device to an organizational PC	5.3	1.46	0.14	< .001***

†Estimates for this indicator not reliable and are thus not reported, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Summary

For Research Question 1, SMEs identified the following ten indicators as being the most important: LG1, LG2, LG3, MC1, HT6, EM8, EM7, EM6, EM5, and PS2A. For Research Question 2, the validated indicator categories were technical (unauthorized logon activity, removable media device file activity [open, write, copy, delete] activity, removable media device connection activity, HTTP/online activity, email activity) and psychometric (conscientiousness, openness, neuroticism, agreeableness, extroversion).

For Research Question 4, the most frequently identified top-ranked correlation was between HT5 and HT4.

For Research Question 5, all but LG2 had high percentages of false negatives in the SME-identified indicators. EM8, EM7, and EM6 had the highest percentages of false positives in the SME-identified indicators. For the system identified indicators, EM9 had the highest rate of false positives. LG4 and MF4 had the lowest rate of false positives. For Research Question 6, when considered in bivariate models, the EM9 was the only system-identified indicator that was significantly predictive of odds of being a malicious user. Performance of this indicator activity was associated with lower odds of being a malicious user. When considered in bivariate models, the following SME-identified indicators were significantly predictive of higher odds of being a malicious user: LG2, LG3, and EM6. The following SME-identified indicators were significantly predictive of lower odds of being a malicious user: MC1, EM8, EM6, and EM5. For Research Question 7, the SME-identified most important rankings were confirmed by bivariate logistic regression results for LG3 and LG2 but were not confirmed for most other indicators.

The following chapter will discuss these results in more detail. The strengths and limitations of the study will be examined. Recommendations for future research will be given.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Over a 12 month period, the estimated average cost of an insider threat attack is \$8.76 million (Ponemon, 2018). Insider threat attack continues to be one of today's most challenging cybersecurity issues that is not well addressed by commonly implemented cybersecurity measures (Homoliak, Toffalini, Guarnizo, & Elovici, 2018). Therefore, the main goal of this proposed research study was to design, develop, and validate a proof-of-concept prototype for a malicious cybersecurity insider threat alerting system that will assist in the detection and prediction of malicious insider threat activity using human-centric technical activities, as well as, individual employee psychometric rating scales. This process was conducted by developing the AI-InCyThR proof-of-concept prototype using SME validated technical and psychometric cybersecurity indicators. This study achieved the seven goals by using a three-phased approach. First, using the Delphi method, an expert panel of SMEs validated the most important technical and psychometric cybersecurity indicators that should be used in the detection of malicious cybersecurity insider threat, as well as, rank the cybersecurity indicator categories. Second, using the Delphi method, the previously validated indicator categories were assigned weights and order of importance by the SMEs, and the SMEs identified their preferred top 10 indicator correlations. Finally, the previously validated and weighted indicators were operationalized, and the AI-InCYThR proof-of-concept prototype was used to measure the accuracy of the top 10 SMEs identified cybersecurity indicators.

Discussion

Principally, the results of the study validated the top 10 cybersecurity indicators important in the detection of malicious cybersecurity insider threat: LG1, LG2, LG3, MC1, HT6, EM8, EM7, EM6, EM5, and PS2. These results indicate that cybersecurity practitioners should begin to focus on the detection of anomalies within these areas of user activity and personality factors. The results also indicated that LG1 was a significant predictor of malicious users, where the odds of being a malicious user are 2.74 times higher if the user performs this activity when compared to users who do not perform this activity. The results of this study identified that the most important correlation between user activities are those related to user Internet usage as determined by SMEs identification of when an employee downloads a file from an external HTTP site (HT4), and when an employee downloads a file from an external HTTP site more than 3 times in one day (HT5). This suggests that cybersecurity practitioners should focus on, and tune their monitoring solutions to identify logon policy violations and any violations of the acceptable Internet usage and file download policy within the organization.

Overall, AI-InCyThR was not implied to be effective in comparison to the SMEs overall importance ranking of the cybersecurity indicators used in the detection of malicious cybersecurity insider threats. However, each of the validated indicators were found to be effective in the detection of malicious insider threat activity. Observed effectiveness was implied for the following items: indicator correlations, indicators presented, and relevance of the indicator to malicious insider threat detection. Observed effectiveness was not implied for the following items: organization of the indicators presented, complexity of the indicators presented, ability to effectively identify potential malicious insider threat, ability to make actionable decisions based on the data presented.

A possibly inconsequential limitation of this study is the use of simulated data. Another possible limitation of this study was the analysis of key words and the fine tuning of the key words within the AI-InCyThR system. In the real world, cybersecurity practitioners have the ability to easily fine tune their monitoring solutions based on organizational policy and real-time threats as they arise.

Implications

The implications of this research study in relation to the existing body of knowledge are the contributions to IS and InfoSec. This study developed and validated a set of cybersecurity indicators for the detection of malicious cybersecurity insider threat activities. One of the major challenges in cybersecurity is the human-centric factor. Because of human nature, some employees won't adhere to acceptable use policies, contributing to cybercrime in ways such as opening attachments containing malware, or using easy to guess passwords, in addition to, an employee leaving and either steals information or compromises systems (Grossbart, 2018).

This study identified SME validated technical and psychometric cybersecurity indicators, how the indicators correlate with each other, as well as, validated indicator effectiveness in the detection of malicious cybersecurity insider threats. This study provides organizations with a set of technical and psychometric indicators that are perceived as effective in the detection of malicious cybersecurity insider threat activities. This set of cybersecurity indicators could assist organizations in the detection and mitigation of malicious cybersecurity insider threat activities.

Recommendations and Future Research

This study was a developmental research and delineated the research approach to employing the Delphi technique to validate and measure cybersecurity indicators, as well as, construct a proof-of-concept prototype to apply the cybersecurity indicators to be used by organizations in the detection of malicious cybersecurity insider threat. The approach illustrated in this research study can be implemented by other fields of study to propose and validate indicators for use in other specialties. Furthermore, this approach can be conveyable to other fields of study were a proof-of-concept prototype needs to be developed.

This research study provides many opportunities for future research studies to be conducted. First, the AI-InCyThR proof-of-concept prototype can be used with real data, where a more robust analysis can be conducted and the technical and psychometric indicators can be more closely examined. Second, the proof-of-concept prototype is SAS code based. Future studies can develop other alternatives to perform the data mining procedures, or create an API that would facilitate the use of the tool. Third, further research can be done with word content filtering and artificial intelligence for the use of word context and sentence structure. While an attempt was made to take HTTP visit content and email content into consideration as an insider threat risk factor, many issues arose causing an extreme level of false positives, resulting in key word identification and content filtering being dropped as a risk factor. Forth, while the Big Five trait model has been widely used in IS research, other studies suggest that it does not completely account

for individual differences in personality and human behavior specifically traits around anti-social behavior and the Dark Triad personality traits (Withers, Parrish, Terrell, & Ellis, 2017). Future research can dive deeper into socially aversive personality types and their relationship to deviant computer use.

Summary

The research problem addressed by this study is the imminent challenge to mitigating cybersecurity insider threats from employees or contractors who may bring harm to the organization by misusing information systems, computer networks, or data (Sood et al., 2015). Insider threat attacks are more in number and more costly than external attacks (Ambre & Shekolkar, 2015, p. 436). Information security is not just about the implementation of specific technologies to monitor information systems, but also the people and processes that rely on these systems (Bowen et al., 2011). Organizations are sitting on repositories of security relevant data that is not being fully capitalized upon by security practitioners with current information security policies and tools (Early & Stott III, 2015). This study facilitated an increase in the body of knowledge by providing validated indicators and a method to connect and correlate the indicators; in a manner that can shift organizational practices from reactive to proactive security by providing organizations a set of indicators to begin to focus their monitoring efforts. This study addressed a valid problem with practical significance (Terrell, 2015).

The main goal of this research study was to design, develop, and validate a proof-of-concept prototype for a malicious cybersecurity insider threat alerting system that will assist in the detection and prediction of malicious insider threat activity using human-

centric technical activities, as well as, individual employee psychometric rating scales. Building on the works of Agrafiotis, Legg, Goldsmith, and Creese (2014), Costa et al., (2014), Greitzer, Dalton, Kangas, Noonan, and Hohimer (2012), Nostro, Ceccarelli, Bondavalli, and Brancati (2014), Warkentin and Willison (2009), as well as, Greitzer et al., (2009), this work was classified as developmental research. Furthermore, it answers the call to develop a proof-of-concept prototype to assist in the detection of malicious insider threat activity. To achieve the main goal, this research set seven specific goals to address seven specific research questions, using a three-phased approach.

During Phase 1, an exploratory study was conducted using a group of cybersecurity SMEs from the LinkedIn professional network to address the following questions:

RQ1: What are the important cybersecurity indicators validated by the expert panel that can assist in the detection of insider threat activity?

RQ2: What are the expert-validated cybersecurity indicator categories?

First, this study performed an extensive review of literature to establish a list of appropriate cybersecurity technical and psychometric indicators. Next, via anonymous online survey, the Delphi method was used with 46 SMEs to propose and validate a set of indicators that can assist in the detection of insider threat activity. The result of the survey identified the top 10 cybersecurity indicators from both the technical and psychometric indicator categories. These results addressed RQ1. Following, the same anonymous online survey asked the SMEs to validate cybersecurity indicator categories. Therefore addressing RQ2.

In continuing Phase 1, once the SMEs had validated the top 10 cybersecurity indicators and cybersecurity indicator categories, another anonymous online survey was administered to same group of SMEs, with 26 SMEs responding, to address the following research questions:

RQ3: What are the expert-approved weights for the identified cybersecurity indicators?

RQ4: What are the expert-identified most significant correlations between cybersecurity indicators?

The SMEs were presented their top 10 identified cybersecurity indicators and asked to weight the indicators, as to assign order of importance. The cybersecurity indicator weights provided by the SMEs were averaged and accepted as weights for the indicators. The indicator with the highest weight represented employees logging on after hours more than 30% of the time, while the indicator with the lowest weight represented employees receiving emails from an external source, where the body of the email contained a risky word more than 30% of the time. Therefore, addressing RQ3. Similarly, the same anonymous online survey asked to choose the most significant correlations between cybersecurity indicators. The top 10 most frequently identified pairings were retained as significant correlations. Pairings with frequencies less than three were excluded. These results addressed RQ4.

Phase 2 of this research study consisted of the operationalization of the cybersecurity indicators using SAS analytics software, as well as, performing a pre-analysis screening of the dataset. Once the cybersecurity indicators were operationalized, analysis of the dataset was performed to identify each simulated user's activity in relation

to the operationalized indicators. Lastly, once the simulated users activity had been identified, a flat file was create to perform the statistical analysis. Phase 2, of this study asked following research questions:

RQ5a: What cybersecurity indicators were identified in experimental settings to have a high rate of false positives as measured by the AI-InCyThR prototype?

RQ5b: What cybersecurity indicators were identified in experimental settings to have a high rate of false negatives as measured by the AI-InCyThR prototype?

RQ6: What simulated user activity *indicators* were identified by the AI-InCyThR proof-of-concept prototype as significant indicators to identify insider threat activity?

To address research questions 5a, cross tabulations were performed for both the system identified indicators and the SME identified indicators. For the system identified indicators, EM9 had the highest percentage of false positives with 82.29%. For the SME's identified indicators, EM7 had the highest percentage of false positives with 64.01%. Therefore, addressing RQ5a.

In addressing research question 5b, the majority of system identified indicators had a high rate of false negatives, ranging from 71.77% to 100%. Out of the 10 SMEs identified indicators, LG2 had the lowest false negative rate of 15.32%. EM6, and EM5, had the highest false negative rate with 99.19%. It was observed that the rest of the SMEs identified indicators had a high rate of false negatives, ranging from 52.42% to 98.39%. Therefore, addressing RQ5b.

In addressing research question 6, a series of bivariate binary logistic regressions were performed on both the system identified indicators and the SMEs identified indicators to determine the indicators that were significant predictors of malicious users. For the system selected indicators, the bivariate models exhibited EM9 was a significant predictor of being a malicious user, $OR = 0.01, p < .001$. The odds of being a malicious user are 0.01 times lower for users who perform this activity when compared to users who do not perform this activity. The bivariate models also exhibited HT7 was a significant predictor of being a malicious user, $OR = 0.19, p = .001$. The odds of being a malicious user were 0.19 times lower for users who performed this activity when compared to those who do not perform this activity. Additionally, the models exhibited no other significant predictors of malicious users. For the SMEs identified indicators, all the indicators were significantly predictive of increased likelihood of being a malicious user, except for LG1, HT6, and PS2A. Additionally, only LG2 and LG3 had a significant positive relationship to malicious use, whereas, MC1, EM8, EM7, EM6, EM5, had a significant negative relationship with malicious use. The results of HT6 showed greatly inflated estimates and should be treated with caution. In regard to HT6, data analysis proved that only 3 users performed this activity. This seemed questionable and the analysis was run a second time which provided the same result. Therefore, addressing RQ6.

In Phase 3, the SME identified indicators were compared towards their actual significance and OR as reported by bivariate logistic regression to address RQ7.

RQ7: How are the simulated user activity correlations that were identified by the SMEs different than those identified by the AI-InCyThR proof-of-concept prototype as significant to identify insider threat activity?

The result indicated that only LG3 and LG2 validated the SMEs high rating of importance as evident by high odds ratios. This in comparison to the SMEs high rating, and low odd ratios for the other indicators, indicating that the directionality of the relationship as generated by the AI-InCyThR system is opposite of what the SMEs rated. Therefore, addressing RQ7.

This study made several contributions to Information Systems and Information Security body of knowledge by developing a SME validated set of cybersecurity indicators and an effective method for the detection of anomalous activities when mitigating malicious cybersecurity insider threats. Specifically, indicators LG3 and LG2, exhibited being strong predictors of malicious activity, and were consistent with the SMEs rating of strong importance. Of the other system identified indicators, they were either not statistically significant (MC4, MF4, EM2, PS1B, PS3B, PS4B, PS5B, LG1, & PS2A) or significant in the negative direction (EM9, HT7, MC1, EM8, EM7, EM6, & EM5), meaning that employees without the indicators were more likely to be a malicious users, than employees with the indicators (contrary to original expectation).

Additionally, the study resulted in establishing validated weights for the cybersecurity indicators. Moreover, the study provided empirical evidence regarding cybersecurity indicators and indicator categories important in cybersecurity monitoring and response decision-making, and the mitigation of malicious cybersecurity insider threat. Given the complexity of the insider threat phenomenon, the results presented in

this study will provide organizations with empirical evidence that can be leveraged to improve the organizations cybersecurity posture, in an effort to lower the probability of financial, information, and intellectual property losses.

In conclusion, organizations can use the validated cybersecurity indicators of LG3, LG2, to assist in the detection of malicious cybersecurity insider threat activity. AI-InCyThR proof-of-concept prototype addressed the challenge of detecting complex malicious cybersecurity insider threats activity in an unconventional manner by validating indicators and indicator correlations. Additionally, organizations can use the AI-InCyThR proof-of-concept prototype as a model for addressing the issues faced when fine tuning cybersecurity monitoring tools and solutions to identify malicious cybersecurity insider threat activity.

Appendix A

Institutional Review Board Approval Letter



MEMORANDUM

To: **Angel Hueca**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **July 13, 2017**

Re: **IRB #: 2017-438; Title, "Development and Validation of a Proof-of-Concept Prototype for Analytics-based Malicious Cybersecurity Insider Threat in Real-Time Identification System"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

Appendix B

Expert Recruitment Email

Dear Cybersecurity Expert,

We seek your help in providing expert validation for an upcoming doctoral research study. I am a PhD candidate in Information Systems, focused on Cybersecurity, at the College of Engineering and Computing, Nova Southeastern University. My research study seeks to develop a proof-of-concept prototype tool that will determine technical and psychometric indicators as precursors to a malicious cybersecurity insider threat attack. These indicators include email activity, http activity, file access, and psychometric classification. To develop the proof-of-concept prototype tool, I need assistance from experts who have knowledge in cybersecurity for three phases of data collection. Phase 1 of my research requires assistance from experts to validate and assign weights to technical and psychosocial indicators that may be used by tools such as Security Event and Information Management (SIEM) systems or Intrusion Detection Systems (IDS).

An online survey will be used to determine the content of the Phase 1 indicator catalogue. All participants are subject matter experts in this area.

By participating in this study, you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in the study at any time. In the event that you no longer wish to participate in the study, your responses will not be recorded. By participating in this study, you certify that you are over the age of 18 years. If you are willing to participate, please click on the link below for access and completion by [DATE]: [LINK]

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study.

If you wish to receive the findings of the study, please contact me via email and I will provide you with the information about the academic research publication(s) resulting from this study.

Regards,

Angel Hueca, PhD Candidate

E-mail: ah1676@nova.edu

Appendix C

Expert Panel Survey Instrument - Delphi 1



Dear Cybersecurity Expert,

Insider threats continue to be one of the most challenging threat vectors for organizations to mitigate. The impact of insider threat attacks can range from companies going out of business, loss of intellectual property, millions of dollars, to the detriment of critical infrastructures such as electrical power grids, communications, or travel infrastructures. In many insider threat attacks, perpetrators exhibited observable questionable behavior such as disgruntlement, anger, or unreliability, yet coworkers or supervisors did not report the behavior to upper management or human resources personnel. This research offers a practical method for the identification of questionable user activity through the development of a simulated monitoring system utilizing synthesized user data and behaviors. As such, the main goal of this research study is to investigate how different activities or indicators relate as precursors to an insider threat attack.

Please read all the survey questions carefully and select one answer per row. Filling out the survey will take about 15 to 20 minutes. Participating in this survey is completely voluntary and anonymous. No personal information will be collected and the data collected will be used for the purpose of this research only. Completing the survey indicates your voluntary participation in the study.

The survey instrument will be presented as follows: After this initial introduction, two sections for experts to identify technical, and psychometric indicators will be presented, followed by a section for demographic information.

This survey is conducted in affiliation with Nova Southeastern University, including Yair Levy, Ph.D. acting as Primary Investigator and one of his doctoral students; Angel L. Hueca, acting as Co-Investigator.

If you would like to see a summary of the results please send an email to ah1676@nova.edu with the subject line "results requested." If you have any questions please send an email to the above mentioned email address.

Thank you in advance for your time and assistance. Thank you for taking the time to participate in our research study.

Regards,

Angel L. Hueca

Please evaluate the following cybersecurity indicators, indicate their level of importance from, 1-Not at all important to 7-Extremely important, as an indicator for malicious cybersecurity insider threat activity.

* LG1: Employee logs on to different PC's without proper authorization

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* LG2: Employee logs on after-hours without proper authorization

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* LG3: Employee logs on after-hours more than 30% of the time (9 out of 30 days) without proper authorization

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* MC1: Employee connects a removable media device to an organizational PC

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* MC2: Employee disconnects a removable media device from an organizational PC

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* MC3: Employee disconnects a removable media device after a PC shutdown

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * MC4: Employee uses (connect/disconnect) a removable media device more than 3 times in one day

Not at all important	Low importance	Slightly important	Somewhat important	Moderately important	Very important	Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * MF1: Employee opens a file from a removable media device on an organizational PC

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * MF2: Employee writes a file to a removable media device

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * MF3: Employee copies a file to a removable media device

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * MF4: Employee copies a file more than 3 times in one day to a removable media device

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * MF5: Employee deletes a file from a removable media device

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* HT1: Employee visits an external HTTP site

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* HT2: Employee uploads a file to an external HTTP site

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* HT3: Employee uploads a file to an external HTTP site more than 3 times in one day

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* HT4: Employee downloads a file from an external HTTP site

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* HT5: Employee downloads a file from an external HTTP site more than 3 times in one day

Not at all important	Low importance	Slightly important	Somewhat important	Moderately important	Very important	Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* HT6: Employee visits an external HTTP site with risky words identified in the organizational word content filtering technology

Not at all important	Low importance	Slightly important	Somewhat important	Moderately important	Very important	Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM1: Employee sends an email with an attachment to an external domain

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM2: Employee sends more than 5 emails with an attachment to an external domain

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM3: Employee receives an email with an attachment from an external domain

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM4: Employee receives more than 5 emails with an attachment, from an external domain in one day

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM5: Employee sends an internal email with risky words identified in the organizational word content filtering technology

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM6: Employee receives an internal email with risky words identified in the organizational word content filtering technology

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM7: Employee receives an external email with risky word identified in the organizational word content filtering technology

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * EM8: Employee sends an external email with risky words identified in the organizational word content filtering technology

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * DF1: Employee accesses a decoy file or honeypot without proper authorization

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * DF2: A PC accesses a decoy file or honeypot without proper authorization

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **Psychometric: Openness**

PS1: Openness - Personality Traits: Imagination, feelings, actions, ideas

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS1A: Low score on Openness: The employee is practical conventional, prefers routine, pragmatic, data driven

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS1B: High Score on Openness: The employee is curious, independent, creative, receptive

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **Psychometric: Conscientiousness**

PS2: Conscientiousness – Personality Traits: Competence, self-discipline, thoughtfulness, goal driven

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS2A: Low score on conscientiousness: The employee is impulsive, careless, disorganized

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS2B: High score on conscientiousness: The employee is persistent, driven, hardworking, dependable, organized

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **Psychometric: Extroversion**

PS3: Extroversion – Personality Traits: Sociability, assertiveness, emotional expression

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS3A: Low score on Extroversion: The employee is quiet, reserved, withdrawn, reflective

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS3B: High score on Extroversion: The employee is outgoing, warm, seeks adventure

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **Psychometric: Agreeableness**

- PS4: Agreeableness - Personality Traits: The employee is cooperative, trustworthy, good-natured

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS4A: Low score on Agreeableness: The employee is critical, uncooperative, suspicious, competitive, challenging

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- * PS4B: High score on Agreeableness: The employee is helpful, trusting, empathetic, cooperative

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **Psychometric: Neuroticism**

PS5: Neuroticism – Personality Traits: The employee has a tendency towards negative emotions

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **PS5A: Low score on Neuroticism: The employee is calm, even-tempered, secure**

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* **PS5B: High score on Neuroticism: The employee is anxious, unhappy, prone to negative emotions**

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

If you have any comments regarding this indicator list or would like to submit an indicator not listed, please do so in the long answer box.

Please evaluate the following cybersecurity indicator categories provided, rate their importance from; 1-Not at all important to 7-Extremely important; as an indicator category for malicious cybersecurity insider threat activity.

* **Technical: Unauthorized Logon Activity**

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Technical: Removable Media Device Connection Activity

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Technical: Removable Media Device File Activity (Open, Write, Copy, Delete) Activity

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Technical: HTTP/Online Activity

Not at all important	Low importance	Slightly important	Somewhat important	Moderately important	Very important	Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Technical: Email Activity

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Technical: Unauthorized File (Decoy/Honeypot) Access

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Psychometric: Openness

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Psychometric: Conscientiousness

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Psychometric: Extroversion

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Psychometric: Agreeableness

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Psychometric: Neuroticism

1-Not at all important	2-Low importance	3-Slightly important	4-Somewhat important	5-Moderately important	6-Very important	7-Extremely important
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

If you have any comments regarding this indicator category list or would like to submit an indicator category not listed, please do so in the long answer box.

* D1. The Gender You Identify With

- ☐ Male
- ☐ Female

* D2. Age Group

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65-74
- ☐ 75 and over

Appendix D

Expert Panel Survey Instrument - Delphi 2



Dear Cybersecurity Expert,

Thank you for participating in the previous expert panel for this research. With the help of your valuable input, I have determined the expert approved cybersecurity indicators and cybersecurity indicator groupings.

Your help is needed to determine the cybersecurity indicator weights (importance) and cybersecurity indicator correlations (relationships) which you feel are important in the detection of malicious cybersecurity insider threat activity.

* Using the slider for the selected indicator, please select the percentage you give the indicator on a scale of 1 to 100, with 100 being the highest.

Number 1 most significant cybersecurity indicators [indicator 1]

0 100

* Number 2 most significant cybersecurity indicator [indicator 2]

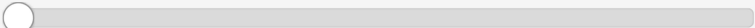
0 100

* Number 3 most significant cybersecurity indicator [indicator 3]

0 100

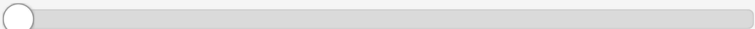
* Number 4 most significant cybersecurity indicator [indicator 4]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

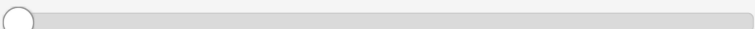
Number 5 most significant cybersecurity indicator [indicator 5]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

Number 6 most significant cybersecurity indicator [indicator 6]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

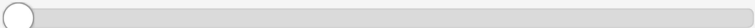
Number 7 most significant cybersecurity indicator [indicator 7]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

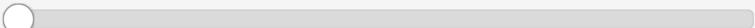
Number 8 most significant cybersecurity indicator [indicator 8]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

Number 9 most significant cybersecurity indicator [indicator 9]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

Number 10 most significant cybersecurity indicator [indicator 10]

0 100

A horizontal slider bar with a circular handle at the 0 position. The bar is light gray with a darker gray track. The numbers 0 and 100 are at the ends.

Please review the indicator matrix below. Identify the 10 most

significant relationships between indicators and select them from the left and right drop-down menus below the image.

Technical: Unauthorized Logon Activity	Technical: Email Activity
LG1: Employee logs on to different PC's without proper authorization	EM1: Employee sends an email with an attachment to an external domain
LG2: Employee logs on after-hours without proper authorization	EM2: Employee sends more than 5 emails with an attachment to an external domain
LG3: Employee logs on after-hours more than 30% of the time (9 out of 30 days) without proper authorization	EM3: Employee receives an email with an attachment from an external domain
Technical: Removable Media Device Connection Activity	EM4: Employee receives more than 5 emails with an attachment, from an external domain in one day
MC1: Employee connects a removable media device to an organizational PC	EM5: Employee sends an internal email with risky words identified in the organizational word content filtering technology
MC2: Employee disconnects a removable media device from an organizational PC	EM6: Employee receives an internal email with risky words identified in the organizational word content filtering technology
MC3: Employee disconnects a removable media device after a PC shutdown	EM7: Employee receives an external email with risky word identified in the organizational word content filtering technology
MC4: Employee uses (connect/disconnect) a removable media device more than 3 times in one day	EM8: Employee sends an external email with risky words identified in the organizational word content filtering technology
Technical: Removable Media Device File Activity (Open, Write, Copy, Delete) Activity	Technical: HTTP/Online Activity
MF1: Employee opens a file from a removable media device on an organizational PC	HT1: Employee visits an external HTTP site
MF2: Employee writes a file to a removable media device	HT2: Employee uploads a file to an external HTTP site
MF3: Employee copies a file to a removable media device	HT3: Employee uploads a file to an external HTTP site more than 3 times in one day
MF4: Employee copies a file more than 3 times in one day to a removable media device	HT4: Employee downloads a file from an external HTTP site
MF5: Employee deletes a file from a removable media device	HT5: Employee downloads a file from an external HTTP site more than 3 times in one day
Psychometric: Openness	Technical: Unauthorized File (Decoy/Honeypot) Access
PS1: Openness - Personality Traits: Imagination, feelings, actions, ideas	DF1: Employee accesses a decoy file or honeypot without proper authorization
PS1A: Low score on Openness: The employee practical conventional, prefers routine, pragmatic, data driven	DF2: A PC accesses a decoy file or honeypot without proper authorization
PS1B: High Score on Openness: The employee is curious, independent, creative, receptive	Psychometric: Conscientiousness
Psychometric: Extroversion	PS2: Conscientiousness – Personality Traits: Competence, self-discipline, thoughtfulness, goal driven
PS3:– Personality Traits: Sociability, assertiveness, emotional expression	PS2A: Low score on conscientiousness: The employee is impulsive, careless, disorganized
PS3A: Low score on Extroversion: The employee is quiet, reserved, withdrawn, reflective	PS2B: High score on conscientiousness: The employee is persistent, driven, hardworking, dependable, organized

PS3B: High score on Extroversion: The employee is outgoing, warm, seeks adventure	Psychometric: Agreeableness
Psychometric: Neuroticism	PS4: Agreeableness - Personality Traits: The employee is cooperative, trustworthy, good-natured
PS5: Neuroticism – Personality Traits: The employee has a tendency towards negative emotions	PS4A: Low score on Agreeableness: The employee is critical, uncooperative, suspicious, competitive, challenging
PS5A: Low score on Neuroticism: The employee is calm, even-tempered, secure	PS4B: High score on Agreeableness: The employee is helpful, trusting, empathetic, cooperative
PS5B: High score on Neuroticism: The employee is anxious, unhappy, prone to negative emotions	

Please review the indicator matrix. Identify the 10 most significant relationships between indicators and select them from the left and right drop-down menus.

	Most Significant Cybersecurity Indicator 1	Most Significant Cybersecurity Indicator 2
Number 1 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 2 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 3 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 4 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 5 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 6 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 7 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>
Number 8 Most Significant Cybersecurity Indicator Correlation	<input type="text"/>	<input type="text"/>

	Most Significant Cybersecurity Indicator 1	Most Significant Cybersecurity Indicator 2
Number 9 Most Significant Cybersecurity Indicator Correlation	<div></div>	<div></div>
Number 10 Most Significant Cybersecurity Indicator Correlation	<div></div>	<div></div>

References

- Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. *Proceedings of the 6th ACM SIGCOMM on Internet Measurement - IMC '06*, 1–12. <http://doi.org/10.1145/1177080.1177086>
- Adams, C. (2011). Identification. In H. van Tilborg & S. (Eds. . Jajodia (Eds.), *Encyclopedia of cryptography and security* (pp. 596–596). Boston, MA: Springer.
- Agrafiotis, I., Legg, P., Goldsmith, M., & Creese, S. (2014). Towards a user and role-based sequential behavioural analysis tool for insider threat detection. *Journal of Internet Services and Information Security (JISIS)*, 4(4), 127–137.
- Alexandrov, T., Bianconcini, S., Dagum, E. B., Maass, P., & McElroy, T. S. (2012). *A review of some modern approaches to the problem of trend extraction. Econometric Reviews* (Vol. 31).
- Alias, N. A. (2015). Designing, developing and evaluating a learning support tool: A case of design and development research (DDR). *SAGE Research Methods Cases Part 1*. <http://doi.org/10.4135/978144627305014558820>
- Almehmadi, A., & El-khatib, K. (2014). On the possibility of insider threat detection using physiological signal monitoring. In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14)* (pp. 1–8). Glasgow, Scotland, UK: ACM. <http://doi.org/10.1145/2659651.2659654>
- Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, 45, 436–445. <http://doi.org/10.1016/j.procs.2015.03.175>
- Ambusaidi, M. A., Tan, Z., He, X., Nanda, P., Lu, L. F., & Jamdagni, A. (2014). Intrusion detection method based on nonlinear correlation measure. *International Journal of Internet Protocol Technology*, 8(2/3), 77–86. <http://doi.org/10.1504/IJIPT.2014.066377>
- Andersen, D., Moore, A. P., Stanton, J. M., Cappelli, D. M., Rich, E., Weaver, E. a, ... Shimeall, T. J. (2004). Preliminary system dynamics maps of the insider cyber-threat problem. In *Proceedings of the 22nd International Conference of the Systems Dynamics Society. Oxford, England.* (pp. 1–36). Oxford, England.
- AT&T Security. (2015). What Every CEO needs to know about cybersecurity: Decoding the adversary. *AT&T Cybersecurity Insights*, 1, 1–36.
- Awan, M. S. K., Burnap, P., & Rana, O. (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *Computers and Security*, 57, 31–46. <http://doi.org/10.1016/j.cose.2015.11.003>

- Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, 30(August), 413–438.
- Band, S., Cappelli, D. M., Fischer, L., Moore, A. P., Shaw, E. D., & Trzeciak, R. (2006). Comparing insider it sabotage and espionage: A model-based analysis. *Technical Report: CERT Program, Software Engineering Institute*, (December), 1–90. Retrieved from <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA459911>
- Barrick, M. R., & Mount, M. K. (1993). Autonomy as a moderator of the relationships between the big five personality dimensions and job performance. *Journal of Applied Psychology*, 78(1), 111–118. <http://doi.org/10.1037/0021-9010.78.1.111>
- Barse, E. L., Kvarnstrom, H., & Johnson, E. (2003). Synthesizing test data for fraud detection systems. *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, 384–394. <http://doi.org/10.1109/CSAC.2003.1254343>
- Bishop, C. M. (2006). *Pattern recognition and machine learning*. New York, NY: Springer Science+Business Media.
- Bishop, M., & Gates, C. (2008). Defining the insider threat. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, (ACM), 1–4.
- Bishop, M., Nance, K., & Claycomb, W. (2017). Inside the insider threat (introduction). In *Proceedings of the 50th Hawaii International Conference on System Sciences | 2017 Inside* (p. 2637). <http://doi.org/10.1109/HICSS.2016.342>
- Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1–16. Retrieved from <http://www.jstor.org/stable/3250956>
- Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. *IEEE International Conference on Technologies for Homeland Security*, 230–235. <http://doi.org/10.1109/THS.2011.6107876>
- Brennan, T., & Jolo, J. (2015). Open web application security project (OWASP):Top considerations for incident response. New York, NY: OWASP. Retrieved from <http://www.proactiverisk.com/wp-content/uploads/2015/06/IR-Guidance.pdf>
- Brown, D. J., Suckow, B., & Wang, T. (2002). *A survey of intrusion detection systems*. Department of Computer Science, University of California, San Diego. San Diego, CA.

- Brunetti, J. M., Auer, S., García, R., Klímek, J., & Nečaský, M. (2013). Formal linked data visualization model. *Proceedings of International Conference on Information Integration and Web-Based Applications & Services - IIWAS '13*, 2, 1–16. <http://doi.org/10.1145/2539150.2539162>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), 523-A7. <http://doi.org/10.1093/bja/aeq366>
- Campbell, D. T. (1957). Factors relevant to the validity of experiments in social settings. *Psychological Bulletin*, 54(4), 1–13.
- Carlin, J. P. (2016). Detect, disrupt, deter: A whole-of-government approach to national security threats. *Havard National Security Journal*, 7, 391–436.
- Carson, J. S. (1986). Convincing users of model's validity is challenging aspect of modelers job. *Industrial Engineering*, 18(8), 74–85.
- Chatfield, C., & Yar, M. (1988). Holt-winters forecasting: Some practical issues. *Journal of the Royal Statistical Society. Series D (The Statistician)*, 37(2), 129–140. Retrieved from <http://www.jstor.org/stable/2348687>
- Chen, M.-S., Han, J., & Yu, P. S. (1996). Data mining: An overview from a database perspective. *IEEE Transactions on Knowledge and Data Engineering*, 8(6), 866–883.
- Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 30, 719–731. <http://doi.org/10.1016/j.cose.2011.08.004>
- Christ, J. (2007). *Web based attacks*. SANS Institute InfoSec Reading Room. Retrieved from <https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053>
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Special publication 800-61, revision 2, Computer security incident handling guide: Recommendations of the national institute of standards and technology, 2, 1–79. <http://doi.org/10.6028/NIST.SP.800-61r2>
- Claycomb, W. R., Legg, P. A., & Gollmann, D. (2013). Guest editorial: Emerging trends in research for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA)*, 5(1), 1–5.
- Clifton, C., & Marks, D. (1996). Security and privacy implications of data mining. *Data Mining and Knowledge Discovery*, 15–19. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.28.891&rep=rep1&type=>

pdf

- Collins, K. M. T., Onwuegbuzie, A. J., & Sutton, I. L. (2006). A model incorporating the rationale and purpose for conducting mixed-methods research in special education and beyond. *Learning Disabilities: A Contemporary Journal*, 4(1), 67–100.
- Committee on National Security Systems. (2013). *Enterprise audit management instruction for national security systems*. Washington, D.C.
- Costa, D. L., Collins, M. L., Perl, S. J., Albrethsen, M. J., Silowash, G. J., & Spooner, D. L. (2014). An ontology for insider threat indicators development and applications. In *9th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2014)* (pp. 1–6). Fairfax, VA: Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA.
- Creasy, J., & Glover, I. (2015). *Cyber security monitoring and logging guide* (1st ed.). Berkshire, United Kingdom: Abbey House.
- Creswell, J. W. (2002). *Education research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.). Boston, MA: Pearson Higher Education.
- Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). Insider threat study: Illicit cyber activity involving fraud in the u. s. financial services sector. *Special Report: CERT Program*.
- Dalkey, N. C., & Helmer, O. (1963). An experimental application of the delphi method to the use of experts. *Management Science*, 9(3), 458–467.
- Danacica, D. (2017). Methodological and applicative problems of using pearson correlation coefficient in the analysis of socio-economic variables. *Romanian Statistical Review*, (2), 148–162.
- Davis, P. k. (1992). Generation concepts and methods of verification, validation and accreditation (VV&A) for military simulations: R-4249-ACQ. Santa Monica, CA: RAND National Defense Research Institute.
- Dawes, R. M. (1979). The robust beauty of improper linear models in decision making. *American Psychologist*, 34(7), 571–582. Retrieved from <http://www.niaoren.info/pdf/Beauty/9.pdf>
- DeYoung, C. G. (2015). Cybernetic big five theory. *Journal of Research in Personality*, 56, 33–58. <http://doi.org/10.1016/j.jrp.2014.07.004>
- Early, G., & Stott III, W. (2015). Preemptive security through information analytics. *Information Security Journal: A Global Perspective*, (June), 1–9. <http://doi.org/10.1080/19393555.2015.1042600>

- Efron, B. (1979). Bootstrap methods: Another look at the jackknife. *The Annals of Statistics*, 7(1), 1–26. <http://doi.org/10.1214/aos/1176344552>
- Efron, B., & Gong, G. (1983). A leisurely look at the bootstrap, the jackknife, and cross-validation. *American Statistician*, 37(1), 36–48. <http://doi.org/10.1080/00031305.1983.10483087>
- Efron, B., Halloran, E., & Holmes, Su. (1996). Bootstrap confidence levels for phylogenetic trees. *Proceedings of the National Academy of Sciences of the United States of America*, 93 VN-r(23), 13429–13434. <http://doi.org/10.1073/pnas.93.23.13429>
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323–.
- Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of Informing Science & IT Education Conference (InSITE)*, (10), 107–118. Retrieved from <http://proceedings.informingscience.org/InSITE2010/InSITE10p107-118Ellis725.pdf>
- Eslahi, M., Salleh, R., & Anuar, N. B. (2013). Bots and botnets: An overview of characteristics, detection and challenges. *Proceedings - 2012 IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2012*, 349–354. <http://doi.org/10.1109/ICCSCE.2012.6487169>
- Few, S. (2007). Data visualization: past, present, and future. *IBM Cognos Innovation Center for Performance Management*, 3–11. Retrieved from http://perceptualedge.com/articles/Whitepapers/Data_Visualization.pdf
- Firstbrook, P., & Wynne, N. (2015). Magic Quadrant for secure email gateways. *Technical Report G00137641*. Stamford, CT: Gartner Inc.
- Fuchs, L., & Gunter, P. (2010). Reducing the risk of insider misuse by revising identity management and user account data. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA)*, 1–14.
- Fuller, K., & Atlasis, A. (2012). *Quick and effective windows system baselining and comparative analysis for troubleshooting and incident response*. SANS Institute InfoSec Reading Room.
- Garrett, R. K., & Danziger, J. N. (2008). On cyberslacking: workplace status and personal internet use at work. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 11(3), 287–292. <http://doi.org/10.1089/cpb.2007.0146>

- Giannasi, F., Lovett, P., & Godwin, A. N. (2001). Enhancing confidence in discrete event simulations. *Computers in Industry*, 44(2), 141–157. [http://doi.org/10.1016/S0166-3615\(00\)00084-1](http://doi.org/10.1016/S0166-3615(00)00084-1)
- Gingrich, P. (2004). Association between variables. In *Introductory Statistics for the Social Sciences* (pp. 794–835). Saskatchewan, Canada: University of Regina. Retrieved from <http://uregina.ca/~gingrich/text.htm>
- Glasser, J., & Lindauer, B. (2013). Bridging the gap: A pragmatic approach to generating insider threat data. *2013 IEEE Security and Privacy Workshops*, 98–104. <http://doi.org/10.1109/SPW.2013.37>
- Gong, G. (1986). Cross-validation, jackknife, and the bootstrap: Excess error estimation in forward logistic regression. *Journal of the American Statistical Association*, 81(393), 108–113. <http://doi.org/10.1080/01621459.1986.10478245>
- Goodwin, L. D., & Leech, N. L. (2006). Understanding correlation: Factors that affect the size of r. *The Journal of Experimental Education*, 74(3), 249–266. <http://doi.org/10.3200/JEXE.74.3.249-266>
- Gordon, T. J. (2009). The delphi method. *The Millennium Project: Futures Research Methodology v3.0 [CD-ROM]*, 1–29.
- Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the big-five personality domains. *Journal of Research in Personality*, 37(6), 504–528. [http://doi.org/10.1016/S0092-6566\(03\)00046-1](http://doi.org/10.1016/S0092-6566(03)00046-1)
- Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis American Educational Research Association Educational Evaluation and Policy Analysis*, 11(3), 255–274. Retrieved from <http://www.jstor.org/stable/1163620>
- Greitzer, F. L., Dalton, A. C., Kangas, L. J., Noonan, C. F., & Hohimer, R. E. (2012). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2392–2401. <http://doi.org/10.1109/HICSS.2012.309>
- Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security* (pp. 85–113). US: Springer. http://doi.org/10.1007/978-1-4419-7133-3_5
- Greitzer, F. L., Frincke, D. a., & Zabriskie, M. (2010). Social/ethical issues in predictive insider threat monitoring. *Information Assurance and Security Ethics in Complex Systems*, 132–161. <http://doi.org/10.4018/978-1-61692-245-0.ch007>
- Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider

- attacks. *Journal of Strategic Security*, 4(2), 25–48. <http://doi.org/10.5038/1944-0472.4.2.2>
- Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. (2014). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. *EService Journal*, 9(1), 106–139.
- Greitzer, F. L., Kangas, L. J., Noonan, C. F., & Dalton, a C. (2010). Identifying at-risk employees: A behavioral model for predicting potential insider threats. *Pacific Northwest National Laboratory*, 1–46.
- Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *Security & Privacy*, 6(1), 61–64.
- Greitzer, F. L., Paulson, P. R., Kangas, L. J., Franklin, L. R., Edgar, T. W., & Frincke, D. a. (2009). Predictive modeling for insider threat mitigation. *Pacific Northwest National Laboratory*, (April), 1–14. Retrieved from <http://www.pnl.gov/cogInformatics/media/pdf/TR-PACMAN-65204.pdf>
- Grispos, G., William Bradley, G., & Storer, T. (2015). Security incident response criteria: A practitioner's perspective. *Proceeding of the 21st Americas Conference on Information Systems (AMCIS)*, 1–16.
- Gritzalis, D., Stavrou, V., Kandias, M., & Stergiopoulos, G. (2014). Insider threat: Enhancing BPM through social media. *2014 6th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2014 Conference and Workshops*. <http://doi.org/10.1109/NTMS.2014.6814027>
- Grossbart, N. (2018). A Deeper look at current issues in cybersecurity: Rapid growth and changes mean many opportunities for students. Retrieved January 11, 2018, from <https://adastra.fit.edu/blog/floridatechbound/a-deeper-look-at-current-issues-in-cybersecurity/>
- Guido, M. D., & Brooks, M. W. (2013). Insider threat program best practices. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. <http://doi.org/10.1109/HICSS.2013.279>
- Han, J., Kamber, M., & Pei, J. (2012). *Data mining: Concepts and techniques* (3rd ed.). San Francisco, CA: Morgan Kaufman. <http://doi.org/10.1016/B978-0-12-381479-1.00001-0>
- Harris, S. (2013). *All in one CISSP: Exam guide* (6th ed.). New York, NY: McGraw-Hill.
- Hashem, Y., Takabi, H., Ghasemigol, M., & Dantu, R. (2016). Inside the mind of the insider: Towards insider threat detection using psychophysiological signals. *Journal of Internet Services and Information Security*, 6(1), 20–36. <http://doi.org/10.1145/2808783.2808792>

- Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008–1015.
<http://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>
- Hauduc, H., Rieger, L., Takács, I., Héduit, A., Vanrolleghem, P. A., & Gillot, S. (2010). A systematic approach for model verification: application on seven published activated sludge models. *Water Science and Technology*, 61(4), 825–839.
<http://doi.org/10.2166/wst.2010.898>
- Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security*, 4(February 2015), 3–20. <http://doi.org/10.1080/2333696X.2008.10855849>
- Hearst, M. A. (1999). Untangling text data mining. *Proceedings of the 37th Annual Meeting of the Association for Computational Linguistics on Computational Linguistics*, 3–10. <http://doi.org/10.3115/1034678.1034679>
- Helminen, A., Halonen, P., Rankinen, T., Nissinen, A., & Rauramaa, K. (1995). Validity assessment of a social support index, 23(1), 66–74.
- Herzel, H., & Große, I. (1995). Measuring correlations in symbol sequences. *Physica A: Statistical Mechanics and Its Applications*, 216(4), 518–542.
[http://doi.org/10.1016/0378-4371\(95\)00104-F](http://doi.org/10.1016/0378-4371(95)00104-F)
- Hill, C. M., & Malone, L. C. (2004). Using simulated data in support of reserach on regression analysis. In *Proceedings of the 2004 Winter Simulation Conference, Ingalls, R.G., M.D. Rossetti, J.B. Smith, and B.A. Peters (eds.)* (pp. 967–973). Washington, D.C.: The Society for Computer Simulation International.
- Ho, S. M., Booth, C., Fu, H., Baeg, J. H., Timmarajus, S., & Liu, M. (2015). Insider threat: Language-action cues in group dynamics. *SIGMIS-CPR'15 ACM*, 101–104.
- Hoffman, B., Meyer, C., Schwarz, B., & Duncan, J. (1990). Insider crime: The threat to nuclear facilities and programs. Santa Monica.: The RAND Corporation.
- Homoliak, I., Toffalini, F., Guarnizo, J., & Elovici, Y. (2018). Insight into insiders: A Survey of insider threat taxonomies, analysis, modeling, and countermeasures. *CoRR, Abs/1805.01612*.
- HPE Security Research. (2016). *HPE Cyber risk report 2016. Hewlett Packard Enterprise Security Research, Cyber Risk Report 2016*. Retrieved from http://techbeacon.com/sites/default/files/gated_asset/hpe-cyber-risk-report-2016.pdf
- IBM Security. (2016). Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations. *IBM X-Force® Research 2016 Cyber Security Intelligence Index*, 1–19. Retrieved from <http://www-01.ibm.com/common/ssi/cgi->

bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

- Ignall, E. J., Kolesar, P., & Walker, W. E. (1978). Using simulation to develop and validate analytic models: Some case studies. *Operations Research*, 26(2), 237–253. <http://doi.org/10.1287/opre.26.2.237>
- INSA. (2013). A preliminary examination of insider threat programs in the U. S. private sector. *Intelligence and National Security Alliance*, (September), 1–20.
- International Standards Organization. (2011). *International standard, ISO 19011: Guidelines for auditing management systems* (Vol. 2). Geneva, Switzerland.
- Jain, A., Duin, R., & Mao, J. (2000). Statistical pattern recognition: A review. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(1), 4–37. <http://doi.org/10.1109/34.824819>
- Judge, T. A., & Bono, J. E. (2000). Five-factor model of personality and transformational leadership. *Journal of Applied Psychology*, 85(5), 751–765. <http://doi.org/10.1037/0021-9010.85.5.751>
- Kivikunnas, S. (1993). Overview of process trend analysis methods and applications. Oulu, Finland: University of Oulu, Department of Process Engineering.
- Kleijnen, J. P. C., & Deflandre, D. (2005). Validation of regression metamodels in simulation: Bootstrap approach. *European Journal of Operational Research*, 170(1), 120–131. <http://doi.org/10.1016/j.ejor.2004.06.018>
- Klein, J. D. (2014). Design and development research: A rose by another name. *AERA 2014 Conference, Philadelphia, PA*.
- Kohonen, T., Oja, E., Simula, O., Visa, A., & Kangas, J. (1996). Engineering applications of the self-organizing map. *Proceedings of the IEEE*, 84(10), 1358–1384.
- Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2015). *Insider threat detection study*. Tallinn, Estonia. Retrieved from www.ccdcoe.org
- Kugler, R. L. (2009). Deterrence of cyber attacks. In *Cyberpower and national security* (p. 320).
- Kuncheva, L. I. (2004). *Combining pattern classifiers: Methods and algorithms*. Hoboken, NJ: John Wiley & Sons.
- Landau, S. (2013). Making sense from snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy*, (July/August), 54–63.
- Law, A. M. (2009). How to build valid and credible simulation models, 24–33.

- Lawton, G. (2008). New technology prevents data leakage. *Computer*, 41(9), 14–17.
<http://doi.org/10.1109/MC.2008.394>
- Levy, R. C. (2007). Prototype. In *Encyclopedia of Small Business* (3rd ed., pp. 923–924). Detroit, MI: Visible Ink.
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9, 181–211.
<http://doi.org/10.1049/cp.2009.0961>
- Lichvar, B. T. (2011). An empirical investigation of the effect of knowledge sharing and encouragement by others in predicting computer self-efficacy and use of information systems in the workplace by. *Dissertation*, 1–146.
- Lindauer, B., Glasser, J., Rosen, M., & Wallnau, K. (2013). Generating test data for insider threat detectors. *Journal of Mobile Networks, Ubiquitous Computing and Dependable Applications*, 5(2), 80–94.
- Linstone, H. A., & Turnoff, M. (Eds. . (2002). The delphi method: Techniques and applications. In *The Delphi method: Techniques and applications* (pp. 1–616). Reading, MA: Addison-Wesley Publishing Company.
<http://doi.org/10.1142/S0219877009001686>
- Linstone, H. A., & Turoff, M. (2002). *The delphi method techniques and applications. The delphi method techniques and applications*. Reading, MA: Addison-Wesley Publishing Company. <http://doi.org/10.2307/1268751>
- Livingston, G. (2000). How to develop your company's first security baseline standard. Fredricksburg, VA: SANS Institute. Retrieved from
<http://www.giac.org/registration/gsec>
- Lovaas, P. (2009). A comprehensive risk-based auditing framework for small-and-medium-sized financial institutions. *Issues in Information Systems*, X(2), 485–494.
- Luijff, E. (2012). Understanding cyber threats and vulnerabilities. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Hague, The Netherlands: Netherlands Organization for Applied Scientific Research TNO. http://doi.org/10.1007/978-3-642-28920-0_4
- Maggi, F. (2010). Are the con artists back? A preliminary analysis of modern phone frauds. *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, 824–831.
<http://doi.org/10.1109/CIT.2010.156>
- Magklaras, G. B., & Furnell, S. M. (2002). Insider threat prediction tool: Evaluating the

- probability of IT misuse. *Computers and Security*, 21(1), 62–73.
[http://doi.org/10.1016/S0167-4048\(02\)00109-8](http://doi.org/10.1016/S0167-4048(02)00109-8)
- Mamcenko, J. (2004). Lecture notes on information resources: Part 1 introduction to data modeling and msaccess. Vilnius, Lithuania: Vilnius Gediminas Technical University.
- Martis, M. (2006). Validation of simulation based models: A theoretical outlook. *Electronic Journal of Business Research Methods*, 4(1), 39–46.
- McAdams, D. P., & Pals, J. L. (2006). A new big five: Fundamental principles for an integrative science of personality. *American Psychologist*, 61(3), 204–217.
<http://doi.org/10.1037/0003-066X.61.3.204>
- McCrae, R. R. (2010). The place of the FFM in personality psychology. *Psychological Inquiry*, 21(1), 57–64. <http://doi.org/10.1080/10478401003648773>
- McCrae, R. R., & Costa, P. T. (1991). Adding Liebe und Arbeit: The Full Five-Factor Model and Well-Being. *Personality and Social Psychology Bulletin*, 17(2), 227–232. <http://doi.org/10.1177/014616729101700217>
- McCrae, R. R., & Costa, P. T. (2008). The five-factor theory of personality. In O. P. John, R. W. Robins, & L. A. Pervin (Eds.) (Eds.), *Handbook of personality: Theory and research* (pp. 159–181). New York: Guilford Press.
- McFadzean, E., Ezingear, J.-N., & Birchall, D. (2011). Information assurance and corporate strategy: A delphi study of choices, challenges, and developments for the future. *Information Systems Management*, 28, 102–129.
<http://doi.org/10.1080/10580530.2011.562127>
- Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods* (4th ed.). Glendale, CA: Pyrczak Publishing.
- Metzger, S., Hommel, W., & Reiser, H. (2011). Integrated security incident management - Concepts and real-world experiences. *Proceedings - 6th International Conference on IT Security Incident Management and IT Forensics, IMF 2011*, 107–121.
<http://doi.org/10.1109/IMF.2011.15>
- Meyers, C., Powers, S., & Faissol, D. (2009). Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. ... *National Laboratory (April ...)*, 1–22. <http://doi.org/10.2172/967712>
- Miller, R. G. (1974). The jackknife - a review. *Biometrika*, 61(1), 1–15.
<http://doi.org/10.1093/biomet/61.1.1>
- Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4), 248–

263. <http://doi.org/10.1108/09685221211267639>

- Moore, A. P., Collins, M. L., Mundie, D., Ruefle, R. R., & McIntire, D. M. (2014). *Pattern-based design of insider threat programs pattern-based design of insider threat programs*. Pittsburg, PA.
- Navathe, S. B. (1992). Evolution of data modeling for databases. *Communications of the ACM*, 35(9), 112–123. <http://doi.org/10.1145/130994.131001>
- Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2014). Insider threat assessment: A model-based methodology. In *Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing, (DISCCO'13, September 30 2013, Braga, Portugal)* (pp. 3–12).
- Nurse, J. R. C., Buckley, O., Legg, P. a, Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. <http://doi.org/10.1109/SPW.2014.38>
- Oceja, L., Ambrona, T., Lopez-Perez, B., Salgado, S., & Villegas, M. (2010). When the victim is one among others: Empathy, awareness of others and motivational ambivalence. *Motivation and Emotion*, 34(2), 110–119. <http://doi.org/10.1007/s11031-010-9161-1>
- Okoli, C., & Pawlowski, S. D. (2004). The delphi method as a research tool: An example, design considerations and applications. *Information & Management*, 42(1), 15–29. <http://doi.org/10.1016/j.im.2003.11.002>
- Ollmann, G. (2007). *The vishing guide*. IBM Global Technologies. Armonk, New York. Retrieved from http://www.gupiaoya.com/tools/Miscellaneous/IBM_ISS_vishing_guide.pdf
- Orans, L., & Firstbrook, P. (2015). Magic quadrant for secure web gateways. *Technical Report G00328904*. Stamford, CT: Gartner Inc. Retrieved from <http://www.gartner.com/technology/reprints.do?id=1-1FTQ83E&ct=130530&st=sb>
- Orloff, J., & Bloom, J. (2014). Bootstrap confidence intervals. *MIT OpenCourseware 18.05*, 11.
- Pare, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information and Management*, 52(2), 183–199. <http://doi.org/10.1016/j.im.2014.08.008>
- Patrick, W. F. (2001). Understanding intrusion dection systems. *SANS Institute*, (May).
- PhridviRaj, M. S. B., & GuruRao, C. V. (2014). Data mining – past, present and future – a typical survey on data streams. *Procedia Technology*, 12, 255–263. <http://doi.org/10.1016/j.protcy.2013.12.483>

- Pilling, R. (2013). Global threats, cyber-security nightmares and how to protect against them. *Computer Fraud and Security*. [http://doi.org/10.1016/S1361-3723\(13\)70081-2](http://doi.org/10.1016/S1361-3723(13)70081-2)
- Ponemon. (2018). *2018 Cost of insider threats : Global*. Traverse City, MI.
- Proctor, P. E., & Mogull, R. (2006). Magic quadrant for content management and filtering. *Technical Report G00137641*. Stamford, CT: Gartner Inc.
- Punithavathani, S. D., Sujatha, K., & Jain, M. (2015). Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Computing*, 18(1), 435–451. <http://doi.org/10.1007/s10586-014-0403-y>
- Pytlik Zillig, L. M., Hemenover, S. H., & Dienstbier, R. A. (2002). What do we assess when we assess a big 5 trait?: A content analysis of the affective, behavioral, and cognitive processes represented in big 5 personality inventories. *Personality and Social Psychology Bulletin*, 28(6), 847–858. Retrieved from <http://journals.sagepub.com.ezproxylocal.library.nova.edu/doi/pdf/10.1177/0146167202289013>
- Raj, M. P., Swaminarayan, P. R., Saini, J. R., & Parmar, D. K. (2015). Applications of pattern recognition algorithms in agriculture : A review. *International Journal of Networking and Applications*, 6(5), 2495–2502.
- Ramim, M. M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small University. *Journal of Cases on Information Technology*, 8(4), 24–34. <http://doi.org/10.4018/jcit.2006100103>
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Mangement*, 2(1), 122–136.
- Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. *Finance*, 38(June), 3–14. <http://doi.org/10.1080/07321870590933292>
- Reddy, C. K., & Aziz, M. S. (2010). Modeling local nonlinear correlations using subspace principal curves. *Statistical Analysis and Data Mining*, 3(5), 332–349. <http://doi.org/10.1002/sam>
- Reilly, A. C., Staid, A., Gao, M., & Guikema, S. D. (2016). Tutorial: Parallel Computing of Simulation Models for Risk Analysis. *Risk Analysis*, 36(10), 1844–1854. <http://doi.org/10.1111/risa.12565>
- Riley, S. (2010). *Science of cyber-security. The MITRE Corporation: JASON Program*.
- Roccas, S., Sagiv, L., Schwartz, S. H., & Knafo, A. (2002). The big five personality

- factors and personal values. *Personality and Social Psychology Bulletin*, 28(6), 789–801. <http://doi.org/10.1177/0146167202289008>
- Roulston, M. S. (1999). Estimating the errors on measured entropy and mutual information. *Physica D: Nonlinear Phenomena*, 125(3–4), 285–294. [http://doi.org/10.1016/S0167-2789\(98\)00269-3](http://doi.org/10.1016/S0167-2789(98)00269-3)
- Rovai, A. P., Baker, J. D., & Ponton, M. K. (2013). Parametric tests: Pearson product-moment correlation test. In *Social Science Research Design and Statistics: A Practitioner's Guide to Research Methods and IBM SPSS Analysis* (2nd ed., pp. 397–403). Chesapeake, VA: Watertree Press.
- Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy*, 12(5), 16–26. <http://doi.org/10.1109/MSP.2014.89>
- Rutkowska, J. (2006). Introducing stealth malware taxonomy. *COSEINC Advanced Malware Labs*, (November), 1–9.
- Salkind, N. J. (2010). *Encyclopedia of research design: Volume 1*. SAGE Publications (1st ed.). Thousand Oaks, CA: SAGE Publications. <http://doi.org/10.4135/9781412961288>
- Santos, O. (2007). Identifying and classifying security threats. In *End-to-end network security: Defense-in-depth* (pp. 99–139). Indianapolis, IN: Pearson Education, Cisco Press.
- Sathya, R., & Abraham, A. (2013). Comparison of supervised and unsupervised learning algorithms for pattern classification. *International Journal of Advanced Research in Artificial Intelligence*, 2(2), 34–38. <http://doi.org/10.14569/IJARAI.2013.020206>
- Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) recommendations of the national institute of standards and technology. *Nist Special Publication*, 800–94, 127. Retrieved from <http://www.reference.com/go/http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
- Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risk: An international delphi study. *Journal of Management Information System*, 17(4), 5–36. <http://doi.org/10.1080/07421222.2001.11045662>
- Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. In *Compsec 2002* (pp. 526–531). London.
- Security, A. (2015). What every CEO needs to know about cybersecurity decoding the adversary. *AT&T Cybersecurity Insights*, 1, 1–36.

- Security, D. of H. (2011). Analyst 's desktop binder: Department of homeland security national operations center media monitoring capability desktop reference binder. Washington, D.C.: Department of Homeland Security.
- Sekaran, U. (2003). *Research methods for business: A skills building approach* (4th ed.). Danvers, MA: John Wiley & Sons. <http://doi.org/10.13140/RG.2.1.1419.3126>
- Seuring, S., & Müller, M. (2008). Core issues in sustainable supply chain management - A Delphi study. *Business Strategy and the Environment*, 17(8), 455–466. <http://doi.org/10.1002/bse.607>
- Shimodaira, H. (2016). Cross-validation of matching correlation analysis by resampling matching weights. *Neural Networks*, 75, 126–140. <http://doi.org/10.1016/j.neunet.2015.12.007>
- Silowash, G., Shimeall, T. J., Cappelli, D., Moore, A., Flynn, L., & Trzeciak, R. (2012). Common sense guide to mitigating insider threats, *4th Editio*(December), 1–144. Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf
- Skinner, R., Nelson, R., Chin, W., & Land, L. (2015). The delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, 37(2), 31–63.
- Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education*, 6(1), 1–21. <http://doi.org/10.1.1.151.8144>
- Sood, A. K., Zeadally, S., Member, S., & Bansal, R. (2015). Exploiting trust: Stealthy attacks through socioware and insider threats. *IEEE Systems Journal*, 1–12.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503–522.
- Specht, S. M., & Lee, R. B. (2004). Distributed denial of service: Taxonomies of attacks, tools and countermeasures. In *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems* (pp. 543–550). <http://doi.org/10.1.1.133.4566>
- Steinparz, S., Abmair, R., Bauer, A., & Feiner, J. (2010). *InfoVis – parallel coordinates. Technology*. Graz, Austria: Graz University of Technology. Retrieved from <http://courses.iicm.tugraz.at/ivis/surveys/ss2010/g3-survey-parcoord.pdf>
- Stone, B. M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society. Series B (Methodological)*, 36(2), 111–147. Retrieved from <http://www.jstor.org/stable/2984809>

- Straub, D. W. (1989). Validating instruments in MIS Research. *MIS Quarterly*, 13(2), 147–169. Retrieved from <http://www.jstor.org/stable/248922>
- Streibel, O. (2008). Trend mining with semantic-based learning. *CEUR Workshop Proceedings*, 358, 71–77.
- Sumsion, T. (1998). The delphi technique. *British Journal of Occupational Therapy*, 61(4), 153–156. <http://doi.org/10.4276/030802212X13383757345102>
- Symantec. (2016). *Internet security threat report. 2016 Internet Security Threat Report* (Vol. 21). Retrieved from <http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947>
- Terrell, S. R. (2015). *Writing a proposal for your dissertation: Guidelines and examples*. Gilford Press. Retrieved from <http://web.b.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzEwNzg5MTNfX0FOO?sid=cb2dea22-46e2-4e64-a428-c76e0cfdbde7@sessionmgr101&vid=5&format=EB&rid=22>
- Thakur, K., Kopecky, S., Nuseir, M., Ali, M. L., & Qiu, M. (2016). An analysis of information security event managers. *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, 210–215. <http://doi.org/10.1109/CSCloud.2016.19>
- The White House. (2010). National insider threat policy minimum standards for executive branch insider threat programs. Washington, D.C.
- Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers and Security*, 24(6), 472–484. <http://doi.org/10.1016/j.cose.2005.05.002>
- Tobergte, D. R., & Curtis, S. (2013). *Statistical. Journal of Chemical Information and Modeling* (Vol. 53). <http://doi.org/10.1017/CBO9781107415324.004>
- Tolman, E. C. (1938). The determiners of behavior at a choice point. *Psychological Review*, 45(1), 1–41. <http://doi.org/10.1037/h0062733>
- Tondel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42–57. <http://doi.org/10.1016/j.cose.2014.05.003>
- Tracey, M. W. (2009). Design and development research: A model validation case. *Educational Technology Research and Development*, 57(4), 553–571. <http://doi.org/10.1007/s11423-007-9075-0>
- Tracey, M. W., & Richey, R. C. (2007). ID model construction and validation: A multiple intelligences case. *Educational Technology Research and Development*.

<http://doi.org/10.1007/s11423-006-9015-4>

- Vaidya, H., Mirza, S., & Mali, N. (2010). Intrusion detection system. *International Journal of Advanced Research in Engineering, Science & Technology*, 3(3), 32. Retrieved from <http://uwcisa.uwaterloo.ca/Biblio2/Year/2010/ACC626 Intrusion Detection Systems E Li.pdf>
- Verizon. (2016). 2016 Data breach investigations report. *Verizon Business Journal*, (1), 1–65. <http://doi.org/10.1017/CBO9781107415324.004>
- Vitak, J., Crouse, J., & LaRose, R. (2011). Personal internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, 27(5), 1751–1759. <http://doi.org/10.1016/j.chb.2011.03.002>
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101–105. <http://doi.org/10.1057/ejis.2009.12>
- Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: The diagnostic work of it security incident response. *Information Management & Computer Security*, 18(1), 26–42. <http://doi.org/10.1108/09685221011035241>
- West, R. (2008). The psychology of security. *Communications of the ACM*, 51(4), 34–41.
- Withers, K. L., Parrish, J. L., Terrell, S., & Ellis, T. J. (2017). The relationship between the “dark triad” personality traits and deviant behavior on social networking sites. *23rd Americas Conference on Information Systems*, 1–10. Retrieved from <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1274&context=amcis2017>
- Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2007). Malware propagation in online social networks: Nature, dynamics, and defense implications categories and subject descriptors. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 196–206. <http://doi.org/10.1145/1966913.1966939>
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing , smishing, & vishing : An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297–307.
- Young, M. D. (2014). National insecurity: The impacts of illegal disclosures of classified information. *ISJLP*, 10, 367–406.
- Young, W. T., Memory, A., Goldberg, H. G., & Senator, T. E. (2014). Detecting unknown insider threat scenarios. *2014 IEEE Security and Privacy Workshops*, 277–288. <http://doi.org/10.1109/SPW.2014.42>